


FORTINET®

NSE Institute

**DO NOT REPRINT
© FORTINET**



FortiClient Study Guide for FortiClient 6.0

DO NOT REPRINT © FORTINET

Fortinet Training

<http://www.fortinet.com/training>

Fortinet Document Library

<http://docs.fortinet.com>

Fortinet Knowledge Base

<http://kb.fortinet.com>

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Support

<https://support.fortinet.com>

FortiGuard Labs

<http://www.fortiguard.com>

Fortinet Network Security Expert Program (NSE)

<https://www.fortinet.com/support-and-training/training/network-security-expert-program.html>

Feedback

Email: courseware@fortinet.com

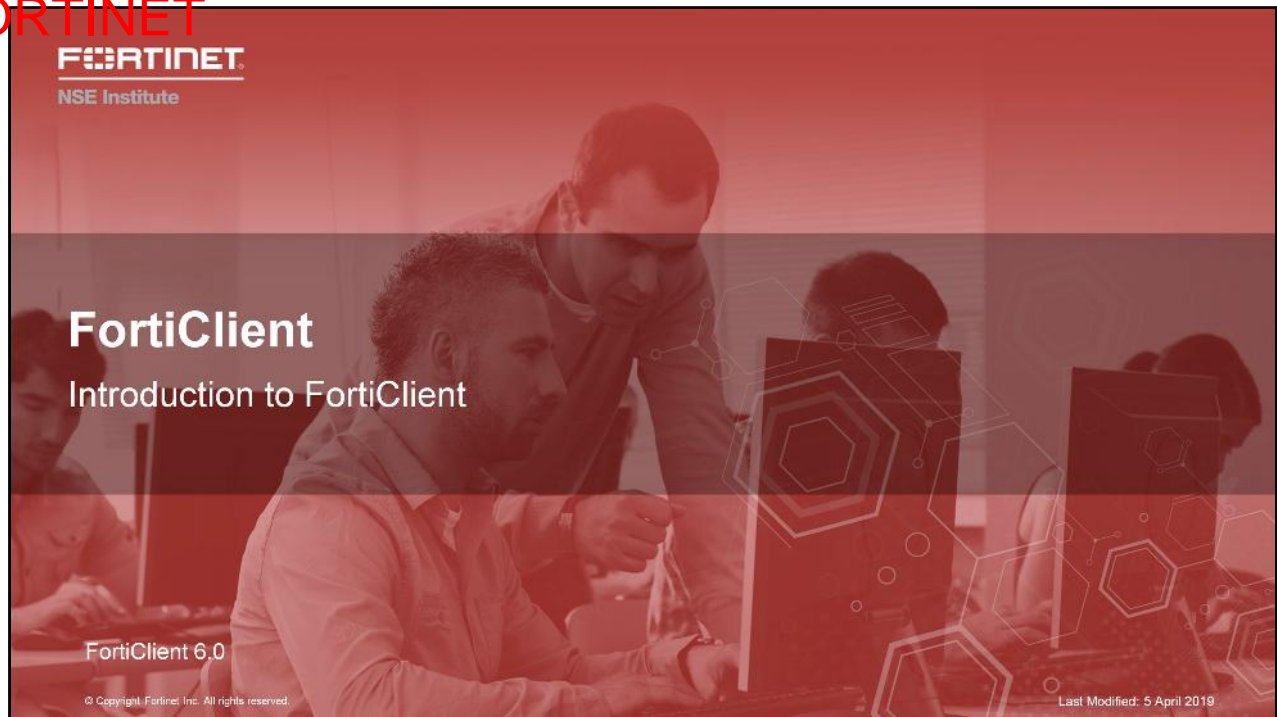


4/8/2019

TABLE OF CONTENTS

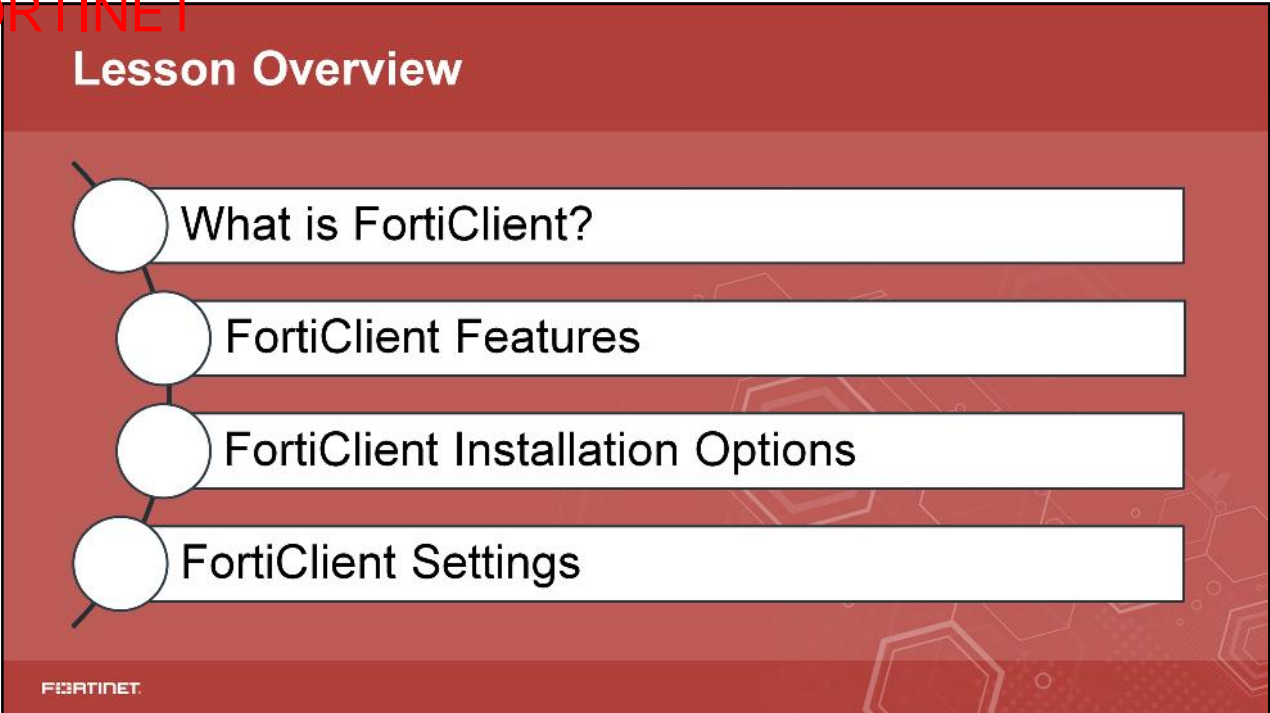
01 Introduction to FortiClient	4
02 Provision and Deploy a Standalone FortiClient	68
03 FortiClient Enterprise Management System (EMS)	98
04 FortiClient Deployment and Provisioning using FortiClient EMS	157
05 Diagnostics and Troubleshooting	207

DO NOT REPRINT
© FORTINET



After completing this lesson, you should have skills that you need to integrate FortiClient into your existing network and manage the security of multiple endpoint devices from a single management console, such as FortiClient Enterprise Management Server (EMS).

DO NOT REPRINT
© FORTINET



Lesson Overview

- What is FortiClient?
- FortiClient Features
- FortiClient Installation Options
- FortiClient Settings

FORTINET

In this lesson, you will learn about the topics shown on this slide.

What is FortiClient?

Objectives

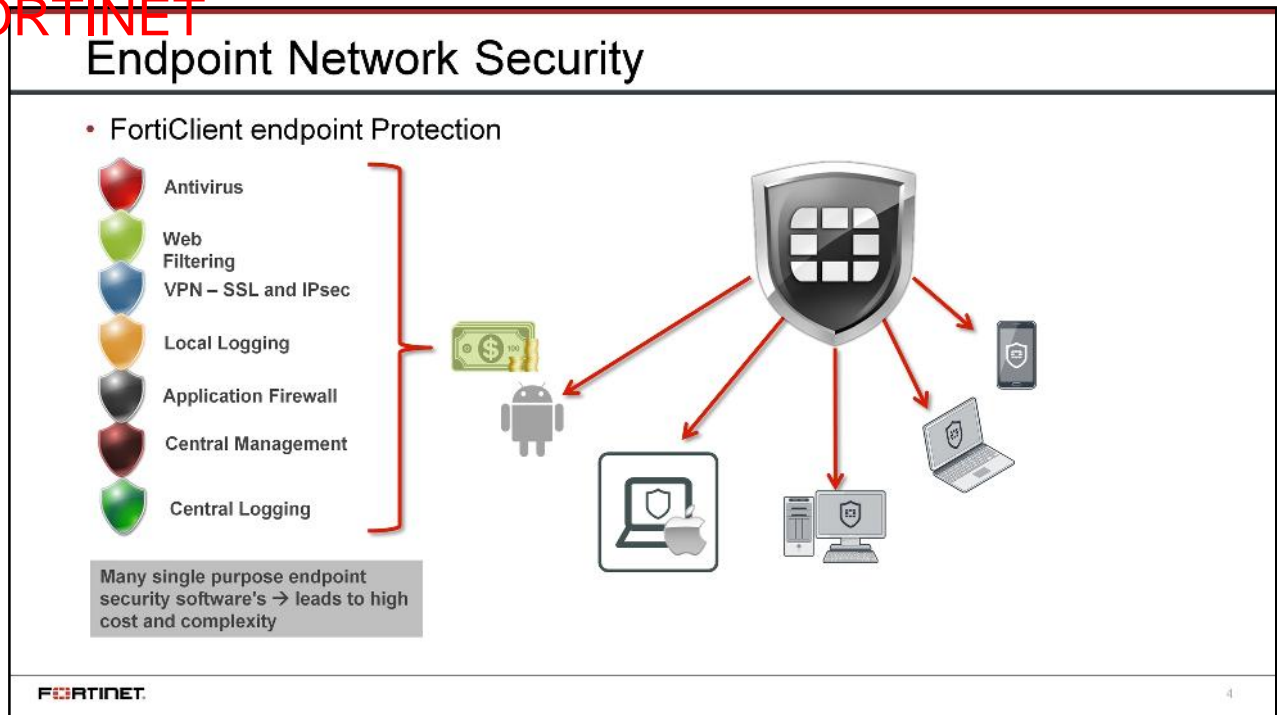
- Know when and why endpoint security is needed
- Identify endpoint security features
- Identify FortiClient modes

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating an understanding of what FortiClient is and what it does, you will be able to understand how FortiClient fits in to your network.

DO NOT REPRINT
© FORTINET



In a typical endpoint network security solution, multiple instances of single-purpose software applications are used. Each application provides a specific service, including:

- Antivirus protection
- Web filtering
- VPN access
- Application firewall

Many endpoint security solutions are not capable of providing central management, central logging, and other features.

When several different applications are used, most times, they all are made by different vendors. Using applications from multiple vendors can introduce unwanted complexity, create many potential points of failure, and increase the cost of initial installation and ongoing operation.

On the other hand, FortiClient offers comprehensive endpoint protection for your Windows-based and Mac-based desktops, laptops, file servers, and mobile devices. FortiClient can safeguard your systems with advanced security technologies and provide a single management console.

DO NOT REPRINT
© FORTINET

Why You Need Endpoint Security

- Traditional antivirus protection is not enough:
 - It cannot stop advanced threats
 - It puts data and organization at risk
 - It doesn't provide central monitoring and visibility into individual endpoints
- Potential threats as well incidents of stolen information and stolen identities are increasing exponentially
- More people are using remote access to connect to work:
 - No control over the remote and mobile devices
 - No control over removable media
- Threats are coming from inside your network:
 - Infected and compromised mobile devices – laptop, removable media
 - Downloading files using VPN
 - Downloading password encrypted files

FORTINET

5

Traditional antivirus software can protect your endpoints from known viruses, but may be unable to detect and protect against advanced threats. This can result in data being lost or compromised. Present day attackers use advanced methods to hijack your identity, such as social media accounts and access your banking information. Sometimes, this information is browser based or application based, and antivirus software can do a little to protect it.

More and more people connect to corporate networks from Wi-Fi hotspots, and providing no control over remote or mobile devices.

Not only do threats come from outside network, people often bring mobile devices inside your network, which may be compromised, and they use your VPN to download files which may contain potential issues.

This is why you need endpoint security!

DO NOT REPRINT
© FORTINET

Endpoint Security

- Protection of an individual workstation or device
- Endpoint security includes a wide range of security features:
 - Malware, grayware, virus, spyware, key logger protection
 - Application firewall
 - Network protection
 - Vulnerability management
 - Input/output data control
 - Central monitoring, provisioning, and logging
- In sync with latest signatures and application updates
- Enforcement of endpoint compliance

FORTINET



Standard security software can provide basic protection, but endpoint security provides basic security plus much more. Endpoint security provides an antivirus program and much more to protect your devices and it creates barrier between your network and the outside. Endpoint security provides antivirus updates, antimalware, IPS/IDS signatures, and updates.

Endpoint security also forces endpoint compliance, which requires endpoints devices to comply with specific criteria before they can gain access to the network.

DO NOT REPRINT
© FORTINET

FortiClient

- Provides a comprehensive network security solution for endpoints while improving your visibility and control:
 - Allows you to manage security of multiple endpoints from the FortiClient Enterprise Management Server (EMS)
 - Allows you to manage endpoints locally or remotely, stationary or mobile from FortiClient EMS
 - Supports multiple platform protection:
 - Windows devices
 - Mac OS devices
 - iOS devices
 - Android mobile devices
- Two modes:
 - Standalone client
 - Managed client

FORTINET

7

FortiClient provides comprehensive endpoint protection for your Windows-based and Mac-based desktops, laptops, file servers, and mobile devices. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

FortiClient enables every device—local or remote, stationary or mobile—to integrate with your FortiGate and FortiClient EMS. FortiClient supports Windows, Mac OS X, iOS, and Android mobile devices, and also integrates your home offices, mobile workers, and visiting partners.

FortiClient can operate in two modes—standalone client and managed client. You will learn about both operating modes in this lesson.

DO NOT REPRINT
© FORTINET

Standalone Client Mode

- A standalone client is not managed and runs in unregistered mode
- Not all features are supported on a standalone client
- Manually defines host security
- FortiGuard services available free of cost
- Standalone clients can be managed and registered to the FortiGate or FortiClient EMS later

FORTINET

8

You can use FortiClient as a standalone client. Standalone client is the free client download that can run in an unregistered mode, delivering a comprehensive solution to devices that are not managed.

Standalone client doesn't support all features. You can register a standalone client to FortiClient EMS, in order to provision full features. You can make configuration changes locally.

DO NOT REPRINT
© FORTINET

Managed Client Mode

- A managed client runs in registered mode
- You can manage a managed client as well as standalone client with the FortiClient EMS
- All the standalone features and additional features are supported
- Enforces endpoint compliance (in integrated mode with FortiGate)
- You can change FortiClient configurations only from the management device

FORTINET

9

In order for the FortiClient to be managed, it needs to be registered to FortiClient EMS. After you have registered the managed client, you can enable additional features, such as application control, vulnerability management, and more, from the FortiClient EMS. You can also enforce endpoint compliance, which forces users to download and install FortiClient and push configuration from FortiClient EMS. On managed clients, configuration changes are grayed out locally on the FortiClient and can be changed only from a managed device.

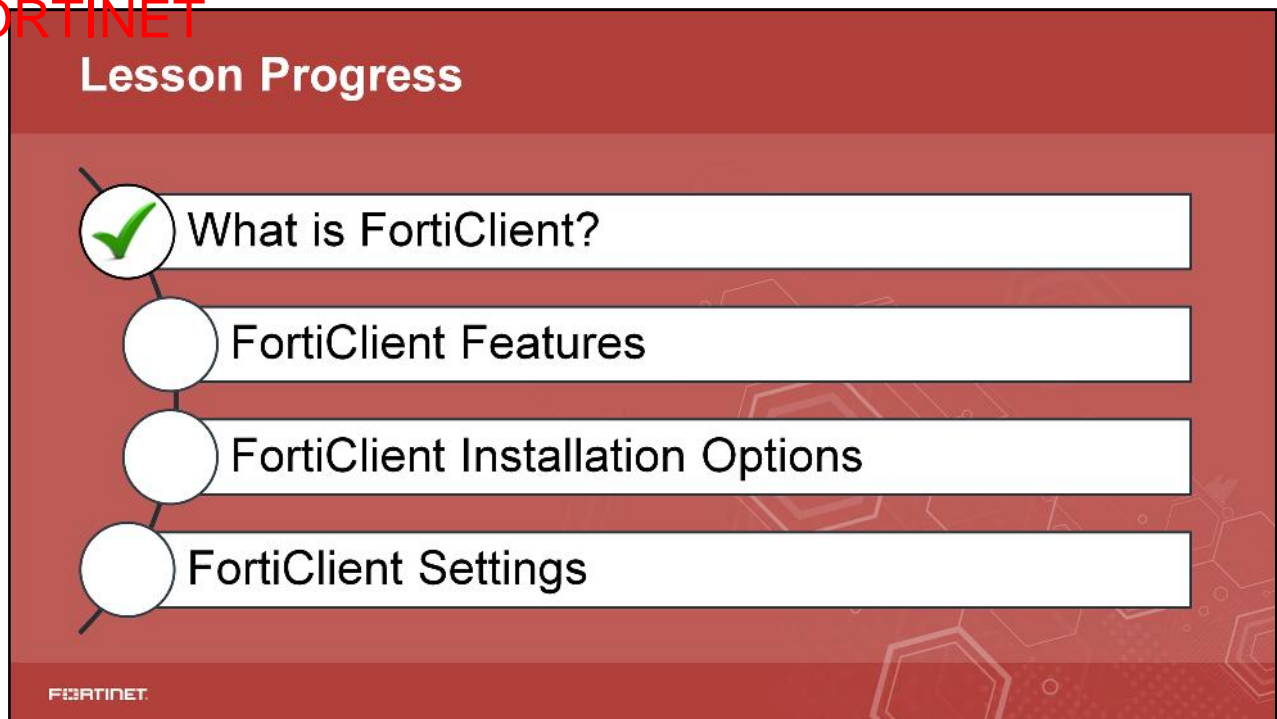
DO NOT REPRINT
© FORTINET

Knowledge Check

1. What is endpoint security?
 - A. Traditional antivirus software
 - ✓ B. A comprehensive network security solution for endpoints

2. Which of the following are the two FortiClient operation modes?
 - ✓ A. Standalone client and managed client
 - B. Standalone client and hybrid client

DO NOT REPRINT
© FORTINET



Good job! You now know more about what FortiClient is and what it does.

Now, you will learn about FortiClient features and what they do.

FortiClient Features

Objectives

- Identify FortiClient key features
- Identify FortiClient standalone client features and managed client features

The Fortinet logo, consisting of the word "FORTINET" in a bold, sans-serif font, with a small red square icon to the left of the text.

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the key features of FortiClient and features of both standalone client and managed client operation modes, you will be able to use FortiClient features and operation modes in your network.

DO NOT REPRINT

© FORTINET

Key Features

- Malware protection (antivirus, antiexploit, and FortiSandbox integration)
- Web security
- Remote access (SSL VPN and IPsec VPN)
- Local logging
- Vulnerability Scan
- Application firewall (managed clients)
- Central management (managed clients)
- Central logging (managed clients)
- Endpoint control (compliance and telemetry)

FORTINET

13

The standalone client (unregistered free version) supports many features. Some of FortiClient features are available on only managed clients (registered clients).

FortiClient key features include:

Malware protection
 Web filtering
 VPN—SSL VPN and IPsec VPN
 Local logging
 Vulnerability scan
 Application firewall (managed client, licensed version only)
 Central management (managed client, licensed Version only)
 Central logging (managed client, licensed version only)

Note that, by default, FortiGate and FortiClient EMS supports up to 10 free clients to be managed. To manage additional clients, you must purchase FortiClient licenses. You will learn more about FortiClient licenses in another lesson.

DO NOT REPRINT
© FORTINET

FortiClient Malware Protection(Antivirus)

- Capable of detecting advanced persistent threats (APT) with FortiSandbox integration:
 - Botnet communication detection
 - Enhanced real-time protection
 - Threat intelligence data to provide dynamic threat detection
- FortiClient can scan:
 - System files
 - Executable files
 - Removable media
 - DLL files and drivers
 - System memory
- File-based malware, malicious websites, phishing, and spam URL protection is included in antivirus protection

FORTINET

14

FortiClient has enhanced capabilities for the detection of APT with FortiSandbox integration. These enhanced capabilities include:

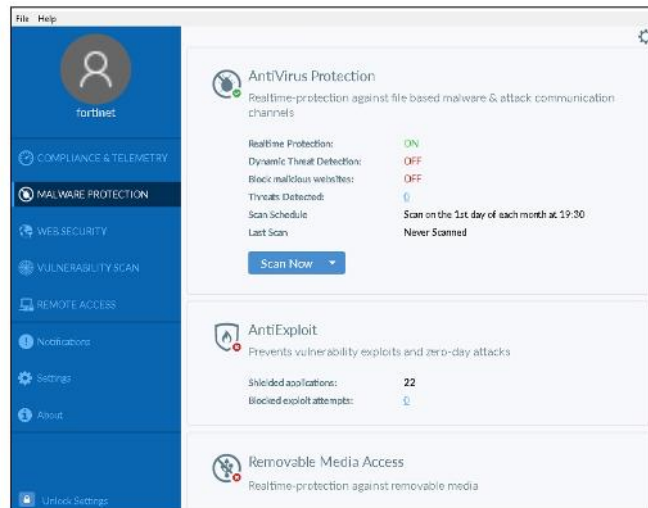
- **Botnet command and control communications detection:** When you enable the botnet feature, FortiClient monitors and compares network traffic on a compromised system with a list of known command and control servers, and blocks it.
- **FortiSandbox integration (Windows only):** You can configure FortiClient to send suspicious files to FortiSandbox, if they could not be detected by local real-time scanning. Access to the downloaded files are blocked until scanning results are returned. As FortiSandbox receives files for scanning, it collects and generates antivirus signatures for such samples. FortiClient periodically downloads the latest antivirus signatures from the FortiSandbox and applies them locally to all real-time, as well as on-demand, antivirus scanning.
- **Enhanced real-time protection implementation (Windows only):** The real-time protection (RTP) feature on FortiClient uses tight integration with Microsoft Windows to monitor files locally or over a network file system, as they are being downloaded, saved, run, copied, renamed, opened, or written to.

FortiClient can scan system files, executable files, removable media, dynamic-link library (DLL) files, memory, and drivers. FortiClient also scans for and remove rootkits. File-based malware, malicious websites, phishing, and spam URL protection is part of the antivirus module.

DO NOT REPRINT
© FORTINET

Antivirus Dashboard

- Settings
 - View and configure real-time protection
 - Show the status of the database
 - Initiate a scan on demand
- By default, only the **Realtime Protection** option is enabled except for Windows Server endpoints



FORTINET

15

Now that you know more about what antivirus capabilities on FortiClient, you will learn more about the available antivirus options.

You can view and configure the real-time protection status, view if database is up-to-date, or perform on-demand antivirus scan.

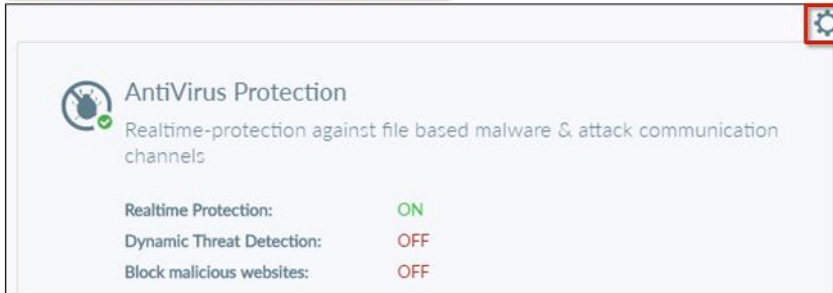
You will learn more about each of these options in detail in this lesson.

DO NOT REPRINT
© FORTINET

Configuring Antivirus Options

- You can click the **Settings** icon to configure
 - Enable real-time protection
 - Schedule a scan
 - Create an exclusion list

Malware Protection > AntiVirus Protection



FORTINET

18

You can click the **Settings** icon to access and configure most of the antivirus options. These options include::

- Realtime Protection:** You can configure settings to specify what to scan. When a virus is detected during real-time monitoring, it will be automatically quarantined. If you have another antivirus program installed, FortiClient will display a warning message stating that your system may lock up or become unstable due to conflicts between the different antivirus products. It is recommended that you uninstall all conflicting antivirus software before installing FortiClient or enabling antivirus real-time protection.
- Scheduled Scan:** You can enable scheduled antivirus scans that will automatically scan your workstation at a scheduled time.
- Exclusions:** You can create an exclusion list that includes files or folders on which you don't want run an antivirus scan.

DO NOT REPRINT
© FORTINET

Configuring Realtime Protection Settings

- You can use real-time protection settings to:
 - Scan files as they are downloaded or copied to my system
 - Block all access to malicious websites
 - You must also enable web filter on FortiClient
 - Block known communication channels used by attackers

Malware Protection > AntiVirus Protection

AntiVirus Protection ☒

Settings

- ☒ Scan files as they are downloaded or copied to my system
- ☐ Dynamic threat detection using threat intelligence data
- ☐ Block malicious websites
- ☐ Block known attack communication channels

Scheduled Scan

Schedule Type: Monthly

Scan On: 1

Start (HH:MM): 19:30

Scan Type: [v]

☐ Disable Scheduled Scan

Exclusions

Add/remove files or folders to exclude from scanning: [Add] [Remove]

FORTINET

17

You can select or clear the following realtime protection settings::

- **Scan files as they are downloaded or copied to my system**
- **Dynamic threat detection using threat intelligence data**
- **Block malicious websites**
- **Block known attack communication channels**

To enable real-time protection, you must select **Scan files as they are downloaded or copied to my system**. Why?

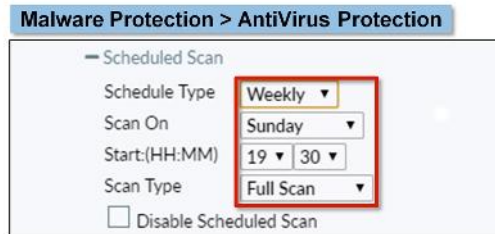
When you download software from the Internet, there is always a chance that you could download applications or programs that will try to inject malware, grayware, or viruses in to your system. To protect your system in real-time, you must enable **Scan files as they are downloaded or copied to my system**.

DO NOT REPRINT
© FORTINET

Configuring Schedule Scan and Exclusions

- You can schedule scans to occur daily, weekly, or monthly and select from these scan types:

- Quick Scan
- Full Scan
- Custom Scan



- You can create an exclusions list and add files and folders that will be excluded from the antivirus scan



FORTINET

18

You can configure daily, weekly, and monthly scans as well as selecting one of the following scan types:

- Quick Scan:** It only scans executable files, DLLs, drivers that are currently running for threats.
- Full Scan:** It performs a full system scan including all files, executable files, DLLs, and drivers for threats.
- Custom Scan:** It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.

All three scan types runs the rootkit detection engine to detect and remove rootkits.

By default, FortiClient is scheduled to run full system scans monthly. It is recommended that you run a full system scan on your endpoint as specified by default setting. Using the default settings provides the best balance between protecting your endpoint from network threats and supporting the best overall performance. If the default settings does not meet your needs, you can always adjust and fine-tune settings accordingly.

Note that if you configure monthly scans to occur on the 31st of each month, the scan will occur on the first day of the month for those months with less than 31 days.

You want to exclude certain files or folders from the antivirus scan, but still want to perform an antivirus scan on rest of the system, you can configure an exclusions list. The files and folders that you add to this list will be excluded from antivirus scanning.

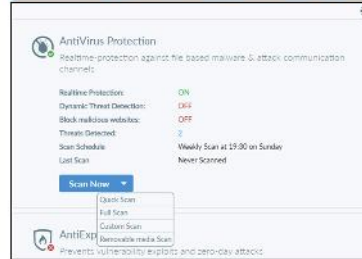
DO NOT REPRINT
© FORTINET

On-Demand Antivirus Scanning

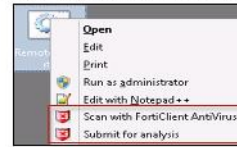
- You can click the Scan Now button to configure on-demand antivirus scanning. You can select from these scan types:

- Custom Scan
- Full Scan
- Quick Scan
- Removable Media Scan

Malware Protection > AntiVirus Protection



- You can scan specific file or folder and submit a file for analysis by right clicking that file on your workstation
 - You can submit up to 5 files a day to FortiGuard for analysis
 - SMTP port is used to upload files



FORTINET

19

You can run on-demand antivirus scan. Scan types include:

Custom Scan

- Runs the rootkit detection engine to detect and remove rootkits. It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats

Full Scan

- Runs the rootkit detection engine to detect and remove rootkits. It then performs a full system scan of all files, executable files, DLLs, and drivers

Quick Scan

- Runs the rootkit detection engine to detect and remove rootkits. It only scans the following items for threats: executable files, DLLs, and drivers that are currently running

Removable Media Scan

- You cannot schedule a removable media scan. A full scan will scan removable media

You can view the date of last scan run. You can perform a virus scan on a specific file or folder on your workstation by right-clicking the file or folder and selecting **Scan with FortiClient AntiVirus** and **Submit for analysis**. You can submit up to five files per day for analysis. FortiClient use SMTP port 25 to upload files, port must be open on network firewall. The FortiGuard team does not provide feedback for the files submitted but creates signatures for the malicious files detected.

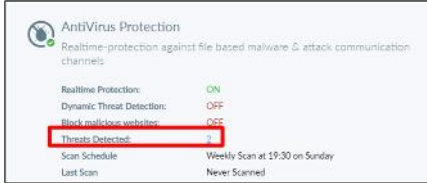
Note that the **Submit for Analysis** option is only available when you select an individual file.

DO NOT REPRINT
© FORTINET

View Threats Detected

- The Threat Detected link allows to view:
 - Quarantined files
 - Site violations
 - Realtime protection events

Malware Protection > AntiVirus Protection



- Viewing quarantined files allows you to view, restore, delete, view logs, or submit the suspicious file to FortiGuard
- When you view site violations, you can view website violations and submit for them for recategorization
- The Realtime Protection link opens `realtime_scan.log`

FORTINET

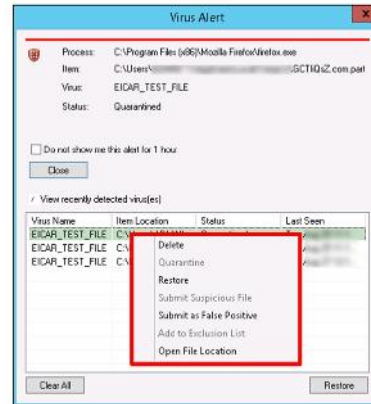
20

The Threat Detection link allows you to view quarantined threats, site violations, and real-time protection events. Each link provides further information about the threat or violation.

- **Quarantined Files:** It allows you to view, restore, or delete the quarantined file. You can also view the original file location, the virus name, submit the suspicious file to FortiGuard, and view logs.
- **Site Violations:** It allows you to view site violations, which are part of FortiClient antivirus, and submit requests to have the site to recategorized. It allows you to view site violation details, including the website name, category, date and time, user name, and status.
- **Realtime Protection events:** When an antivirus real-time protection event occurs, it is logged in `realtime_scan.log` and can be opened in any text editor. By default, realtime protection events open in the default viewer.

Virus Alert

- A warning message opens when a virus is detected while downloading file via web-browser.
 - Automatically quarantine the file
 - Right click on a file to access context menu



FORTINET

21

If FortiClient detects a virus file that is being downloaded through a web browser, FortiClient presents a warning message and automatically quarantines the virus file. If you right-click the quarantined file, you can take the following actions:

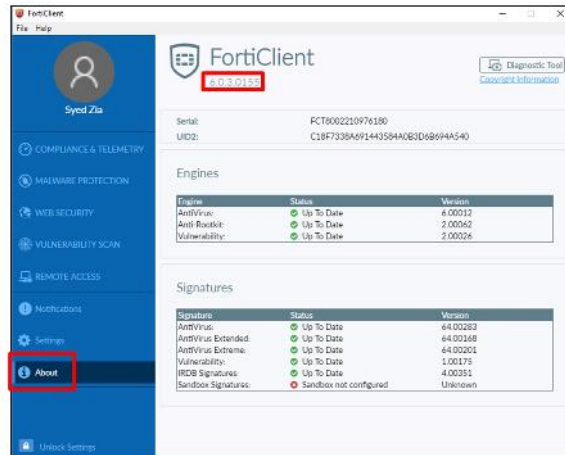
- **Delete:** You can delete a quarantined or restored file.
- **Quarantine:** You can quarantine a restored file.
- **Restore:** You can restore a quarantined file, and also allows you to add to Exclusion list.
- **Submit Suspicious File:** You can submit a file to FortiGuard as a suspicious file.
- **Submit as False Positive:** You can submit a quarantined file to FortiGuard as a false positive.
- **Add to Exclusion List:** You can add a restored file to the exclusion list. Any files in the exclusion list will not be scanned.
- **Open File Location:** You can open the file location on your workstation.

Note that if you did not select the **Alert when viruses are detected**, you will not receive the virus alert dialog box when attempting to download a virus in web browser.

DO NOT REPRINT
© FORTINET

FortiClient Engine and Signature Version

- You can view FortiClient engine and signature versions



FORTINET

22

You can view the current FortiClient version, engine, and signature information by selecting **About**.

You can use FortiManager for client software and signature updates when registered to FortiGate or EMS.

DO NOT REPRINT
© FORTINET

Antiexploit Detection

- Protects vulnerable endpoints from unknown exploit attacks
- FortiClient monitors the behaviour of popular applications, such as web browsers.
 - Internet Explorer
 - Chrome
 - Firefox
 - Opera
- Protects against memory-based attacks and drive-by download attacks



FORTINET

23

The antiexploit detection protects vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behaviour of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, to detect exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, FortiClient terminates the compromised application process.

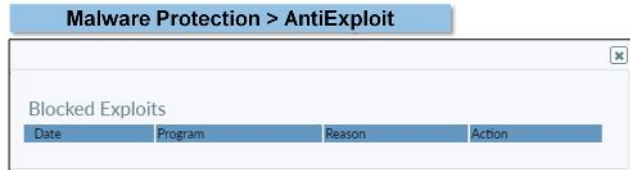
The antiexploit detection feature also protects endpoint from memory-based attacks and drive-by download attacks. It also detects and blocks unknown and known exploit kits.

It is a signature less solution.

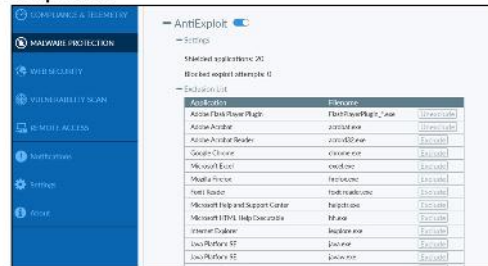
DO NOT REPRINT
© FORTINET

Antiexploit Detection (Contd)

- You can view the exploit attempts FortiClient has blocked



- You can view applications protected from exploits



FORTINET

24

You can determine which applications are protected from exploits based on the buttons beside their names.

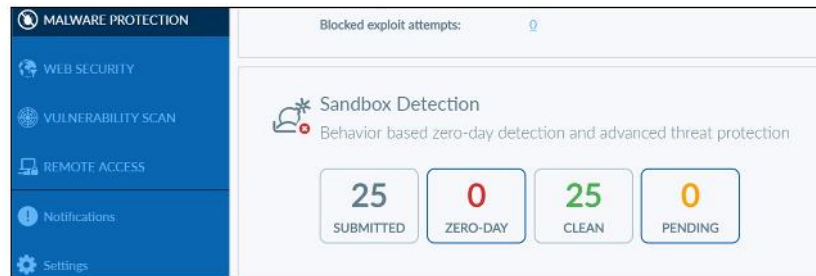
Applications with an **Exclude** button beside their names are protected from evasive exploits.

Applications with an **Unexclude** button beside their names are not protected from evasive exploits. You can protect the application by clicking the **Unexclude** button.

DO NOT REPRINT
© FORTINET

Sandbox Detection

- FortiClient supports integration with FortiSandbox
- FortiClient sends files to FortiSandbox for further analysis if they are not detected locally
- Endpoint users can also manually submit files to FortiSandbox for scanning
- Access to files can be blocked until the FortiSandbox scanning result is returned



FORTINET

28

FortiClient supports integration with FortiSandbox. When configured, FortiSandbox automatically scans files downloaded on the endpoint, or from removable media attached to the endpoint, or mapped network drives. FortiClient also automatically scans files downloaded with an email client on the endpoints, or from the Internet.

In each case, if the file is not detected locally, and FortiSandbox integration is configured, FortiClient sends the file to the FortiSandbox for further analysis. Endpoint users can also manually submit files to FortiSandbox for scanning. Access to files can be blocked until the FortiSandbox scanning result is returned. When scanning is complete, FortiSandbox can quarantine infected files, or alert and notify the endpoint user of infected files without quarantining the files.

DO NOT REPRINT
© FORTINET

Configuring Sandbox Detection

- You can click the **Settings** icon to configure:

- Submission
- Access
- Remediation
- Exceptions



FORTINET

20

You can click the **Settings** icon to access and configure sandbox options. These options include:

- Wait for FortiSandbox results before allowing file access:** Select to wait for FortiSandbox analysis results before files can be accessed.
- Deny Access to file when there is no sandbox result:** Select to deny access to files when FortiClient cannot reach FortiSandbox for file analysis or no result.

You can configure the following FortiSandbox submission options:

- All files executed from mapped network drives:** Select to submit all files that are executed on mapped network drives to FortiSandbox for analysis. Clear the checkbox to disable this feature.
- All files executed from removable media:** Select to submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis. Clear the checkbox to disable this feature.
- All web downloads:** Select to submit all web downloads on the endpoint to FortiSandbox for analysis.
- All email downloads (Ex. Outlook):** Select to submit all email downloads on the endpoint to FortiSandbox for analysis.

You can configure the following remediation options:

- Quarantine infected files:** Select to quarantine infected files.
- Alert & Notify only:** Select to alert and notify the endpoint user about infected files, but not quarantine infected files.

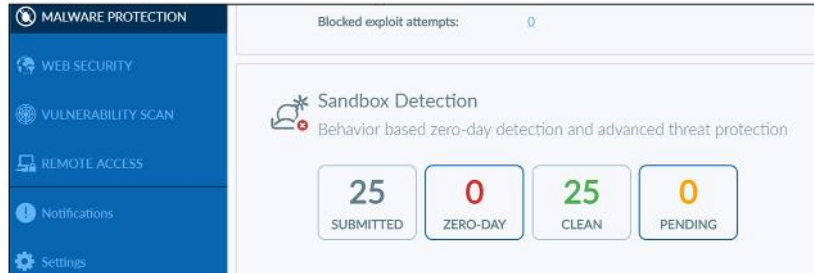
You can configure the following exclusion options:

- Exclude files from trusted sources:** Select to exclude files from trusted sources from FortiSandbox analysis.
- Exempt specified files / folders:** Select to exempt specified files and/or folders from FortiSandbox analysis. You must also create the exclusion list.

DO NOT REPRINT
© FORTINET

On-Demand Scan and Viewing Results

- Scanning with FortiSandbox on demand
- Viewing FortiSandbox scan results



FORTINET

27

You can send files to FortiSandbox for scanning on demand when FortiSandbox is enabled and online.

FortiSandbox scan results display on the **Malware Protection** page. When a virus is detected, FortiClient creates a notification alert that displays the following information:

Submitted: The number of files submitted to FortiSandbox for scanning.

Zero-day: The number of detected zero-day files.

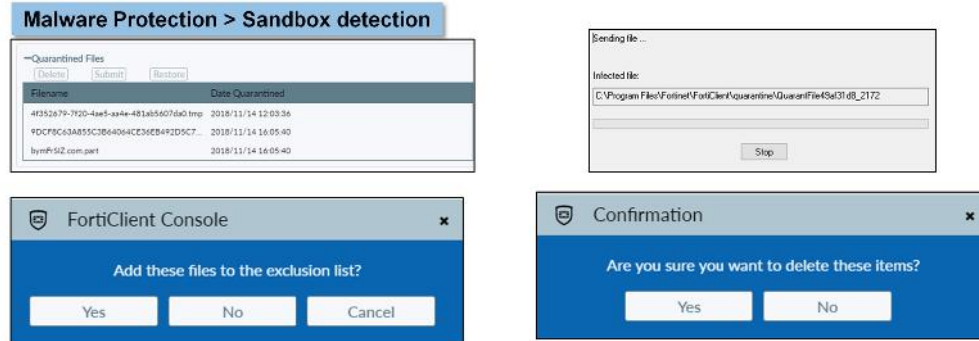
Clean: The number of files determined clean after FortiSandbox scanning.

Pending: The number of files waiting for FortiSandbox scanning.

DO NOT REPRINT
© FORTINET

View, Submit, Restore, and Delete Quarantined Files

- You can view files quarantined by FortiSandbox
- You can also restore and delete quarantined files and submit them for another analysis



FORTINET

28

You can view files quarantined by FortiSandbox. You can also restore and delete quarantined files.

Endpoint users can only restore and delete quarantined files with FortiClient in standalone mode. When you restore a quarantined file, you can choose whether to add the file to the exclusion list. You can submit quarantined files to FortiSandbox for scanning.

The maximum age for quarantined files is specified in the

`<quarantine></quarantine>` XML tags:

```
<forticlient_configuration>
<antivirus>
<quarantine>
<cullage>100</cullage>
</quarantine>
</antivirus>
</forticlient_configuration>
```

The `<cullage>` XML tag specifies how long to hold quarantined files, in days, before deleting them. A number from 1 to 365. Default value is 100 days

Note that you cannot restore and delete quarantined files when FortiClient is in managed mode.

DO NOT REPRINT
© FORTINET

FortiClient Web Security vs Web Filter

- Web Security vs Web Filter
 - Web security is available on the console of an unregistered FortiClient
 - Web filter is available on the console of an registered FortiClient
- When FortiClient is unregistered, you can enable, disable, and configure web security features
- When FortiClient is registered, the web filtering profile is received from FortiGate or EMS and is read only
- Take actions on web traffic based on URL category or custom URL filters – block, allow, warn, or monitor
- FortiGuard distribution network (FDN) handles URL categorization
- Custom URL filter exclusion list overrides FDN

FORTINET

29

On an unregistered (standalone) FortiClient, you can configure web security features on the FortiClient console. On a FortiClient that is registered to FortiGate or EMS, you view the web filtering profile from the FortiClient console.

When FortiClient is not registered to FortiGate or EMS, you can enable or disable web security features. You can define what sites are allowed, blocked, or monitored, and view violations.

When FortiClient is registered to FortiGate or EMS, web filter configuration settings are pushed from the management device and are read only on the FortiClient console.

If FortiClient is registered with FortiGate, you can web filter compliance policy by clicking a **Fix** button that displays on FortiClient.

Web security and web filter features allow you to block, allow, warn, and monitor web traffic based on URL category or custom URL filters. URL categorization is handled by the FDN. You can create a custom URL filter exclusion list which overrides the FDN category.

DO NOT REPRINT
© FORTINET

Configuring Web Security

- Click **Unlock Settings** at the bottom of the page
- You can click the **Settings** icon to configure the following:
 - Web security profile (Site Categories)
 - Exclusion list
 - Settings
 - Violations: view and clear

From FortiClient version 6.0, all the settings are locked by default. You can unlock settings by Clicking **Unlock Settings**.

You can enable and disable web security feature from clicking to toggle between Enable and Disable link. Web security is enabled by default.

You can configure most web security options by clicking the **Settings** icon. Configurable options include:

- Web security profile (site categories)
- Exclusion List
- Settings
- Violations

DO NOT REPRINT
© FORTINET

Configuring Web Security and Exclusions List

- Site categories allow you to:
 - Allow, block, warn, or monitor
 - Right-click a category to select and action



- Exclusion List tab:
 - Allows to add URLs that are overridden from FDN category
 - Three types to choose from—Simple, Wildcard, Regular Expression
 - Three actions to choose from—Block, Allow, Monitor

FORTINET

31

You can configure a web security profile to allow, block, warn, or monitor web traffic based on website categories and subcategories.

Allow: Permits access to the sites within the category.

Block: Prevents access to sites within the category. Users attempting to access a blocked site will receive a replacement message explaining that access to the site is blocked.

Warn: Presents the user with a message, allowing them to continue if they choose. Accepting a disclaimer will allow users to browser the override category for 5 minutes.

Monitor: Permits and logs access to sites in the category. You may also enable user quotas when enabling the monitor action.

What if you want to exempt a URL that is part of category, but you still want to take action on that category as a whole?

You can configure an exclusion list to which you can add websites and set the permissions to allow, block, and monitor. You can configure simple, wildcard, or regular expressions as a type. If the website is part of a blocked category, an allow or monitor permission in the exclusion lists allows the user to access the specific URL.

DO NOT REPRINT
© FORTINET

Web Security—Settings and Violations

- Settings allow you to enable or disable:
 - Site categories
 - Log all URLs
 - Web browser usage and duration
- If **Site Categories** is disabled, the endpoint is protected by the configured exclusion list only
- Violations
 - Allows you to view web security violations
 - FortiGuard Site Categories—only if action is set to block or warn
 - Exclusion list—only if action is set to block

FORTINET

32

When you configure web security settings, you can enable and disable the following:

- **Site Categories:** Allows you to enable or disable FortiGuard categories.
- **Log all URLs:** Logs all URLs with an assigned action. The logged files can be downloaded.
- **Web Browser Usage and Duration:** Allows the FortiClient to record detailed information about the user's web browser activities, such as:
 - A history of websites visited by the user (as shown in regular web browser history)
 - An estimate of the duration or length of stay on the website

Note that when site categories are disabled, FortiClient is protected by the exclusion list only.

You can view site violations and violation details including the website name, category, date and time, and user name. The violation will show only if the actions is set to block or warn for FortiGuard site categories and block for the exclusion list.

DO NOT REPRINT
© FORTINET

VPN—SSL and IPsec

- FortiClient supports both IPsec and SSL VPN
 - Can configure on the FortiClient console
- Simplified VPN configurations
- Supports two-factor authentication with FortiToken
- Allows you to create multiple VPN profiles
- Allows to activate VPN before (Windows and AD environment)



Remote Access

VPN Name	Student_SSL
Username	
Password	
Token	Click on 'FTM Push' or enter token code
<div> <div>FTM Push</div> <div>OK</div> <div>Cancel</div> </div>	

Two-factor authentication with FortiToken

FORTINET

33

FortiClient supports both IPsec and SSL VPN connections to your network for remote access. You can provision client VPN connections in the FortiClient profile (managed client) or configure new connections in the FortiClient console (standalone client).

You can also configure two-factor authentication using FortiToken for enhanced security for both types of VPNs on your FortiGate device for FortiClient VPN connections.

FortiClient VPN features are not limited to basic configuration and provisioning, but can be used for advanced configurations (managed clients). For example, you can automatically connect to a VPN when FortiClient is launched, or you can map or unmap a network drive when tunnel is connected or disconnected, respectively.

You can also configure FortiClient to connect to a VPN before the logging in (either in to a Windows account or through an AD environment).

DO NOT REPRINT
© FORTINET

IPsec VPN

- Easy configuration to create, edit, or delete VPN connection
 - Authentication settings—prompt on login, save login (only username), or disable
 - Allows you to configure VPN settings, phase I, and phase II settings
- Configure many advanced configurations when managed by FortiGate FortiClient EMS
 - Redundant IPsec VPN connections
 - Save password
 - Auto connect
 - Always up

Remote Access > IPsec VPN

Edit VPN Connection

VPN: SSL VPN IPsec VPN

Connection Name:

Description:

Remote Gateway: ✕

[+Add Remote Gateway](#)

Authentication Method: Pre-shared key

Authentication (XAuth): ☒ Prompt on login ☐ Save login ☐ Disable

[+ Advanced Settings](#)

FORTINET

34

You can configure the IPsec VPN configuration directly on the FortiClient console. It allows you to create, edit, save, or delete IPsec VPN. You can create and save multiple IPsec connections. As this configuration is one side of the IPsec VPN, this configuration settings needed to be matched with the FortiGate IPsec configuration in order to connect and access remote resources.

When FortiClient is managed by FortiGate or FortiClient EMS, it allows you provision these configurations along with advanced configurations such as redundant IPsec VPN connections, save password, auto connect, and always up, to name a few.

DO NOT REPRINT
© FORTINET

SSL VPN

- Create, edit, or delete a VPN connection:
 - Save the login information—username
 - Configure authentication—prompt on login, save login (only username), or disable (only when Client Certificate option is enabled)
- When managed by FortiClient EMS, perform advanced configuration:
 - Priority-based SSL VPN connections
 - SSL VPN portal on FortiGate allows
 - Save password
 - Auto connect
 - Always up
- Supports DTLS
 - If required falls back to TCP over TLS
 - Windows Only

Remote Access > IPsec VPN

Edit VPN Connection

VPN: SSL VPN IPsec VPN

Connection Name:

Description:

Remote Gateway: ✕

☒ Add Remote Gateway

☒ Customize port:

Client Certificate: None ▼

Authentication: ☒ Prompt on login ☐ Save login ☐ Do not Warn Invalid Server Certificate

FORTINET

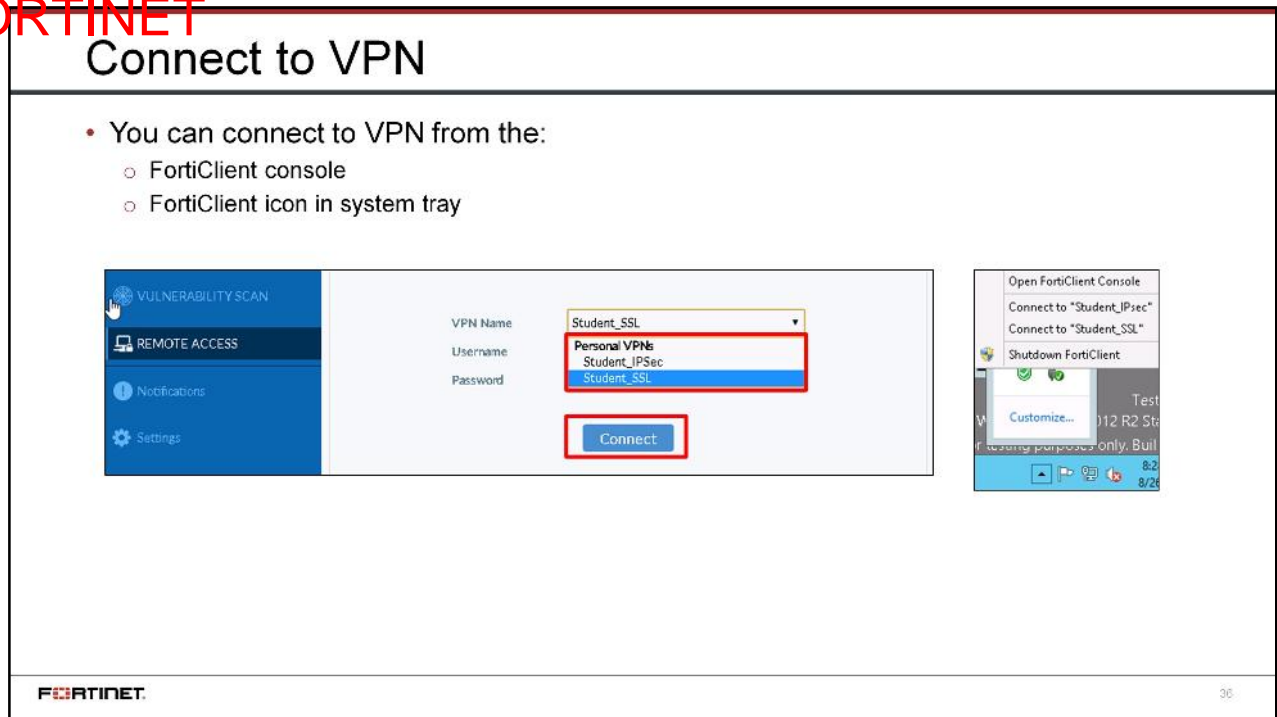
35

The SSL VPN configuration is similar to IPsec configuration where you configure one side of the tunnel and other side is configured on FortiGate.

When FortiClient is managed by FortiGate or FortiClient EMS, it allows you provision these configurations along with advanced configurations on SSL VPN portals, and many more.

DTLS is a Windows only feature, and not recommended for slow or networks.

DO NOT REPRINT
© FORTINET



To connect to a VPN (IPsec or SSL), select the VPN name from the drop-down menu on FortiClient console. Enter your username, password, and then click **Connect**. Optionally, in the system tray, right-click the FortiClient icon and select the VPN connection you want to connect to. When connected, the console will display the connection status, duration, and other relevant information.

Note that provisioned VPN connections will be listed under **Corporate VPN**. Locally configured VPN connections will be listed under **Personal VPN**.

DO NOT REPRINT
© FORTINET

Logging

- Logging
 - VPN, application firewall, antivirus, web filter, update, and vulnerability scan logging
 - View logs locally
 - Export or clear logs
 - Default logging level is Information

Logging Level	Description
Emergency	The system becomes unstable
Alert	Immediate action is required
Critical	Functionality is affected
Error	An error condition exists and functionality could be affected
Warning	Functionality could be affected
Notice	Information about normal events
Information	General information about system operations
Debug	Debug FortiClient

FORTINET

37

You can view the logs locally on FortiClient. Some features logging is only available when registered to FortiGate or FortiClient EMS. You can view VPN, antivirus, web filter, and update logs in standalone client or managed client mode.

Some features, such as application firewall and vulnerability scan requires FortiClient to be managed from FortiGate or FortiClient EMS; therefore, logging is only available when FortiClient is managed by FortiGate or FortiClient EMS.

You can export the log file (.log) in standalone or managed mode, but the option to clear logs is only available only in standalone mode.

FortiClient provides options for logging levels, such as information, notice, or emergency. When FortiClient is managed by FortiGate or FortiClient EMS, you can configure the XML configuration to set the logging levels.

Default logging level on FortiClient is **Information**.

So far, you have learned about mostly the features that are available in standalone client. Now you will learn about the features that are available for managed client mode.

DO NOT REPRINT
© FORTINET

Application Firewall (Managed Clients)

- Application control:
 - Application firewall
 - Block specific application traffic
- FortiClient must be registered to FortiGate or EMS using endpoint control:
 - Disabled by default and tab is hidden for standalone clients
- Read-only profile in the FortiClient console:
 - Allows you to view blocked applications – past 7 days
- Capable of recognizing network activity (application traffic):
 - Allows to create rules to block or allow traffic per application or category

FORTINET

38

You can use the application firewall feature to detect and take actions against network traffic, depending on the application that is generating the traffic. This feature is available on managed clients only. By default, this feature is disabled and hidden for the standalone clients.

Application firewall uses IPS protocol decoders to analyze and detect application traffic even, on non-standard ports.

FortiClient can recognize the traffic generated by a large number of applications. You can create rules to block or allow application traffic on FortiGate or EMS based on the category or application. The rules are then pushed to managed FortiClient.

Application firewall settings are read-only on the FortiClient console. You view blocked applications for the past 7 days.

DO NOT REPRINT
© FORTINET

Vulnerability Management

- Vulnerability management:
 - List of vulnerabilities detected
 - One-click link to install patches and resolve as many identified vulnerabilities as possible
 - List of patches that require manual installation by the endpoint user to resolve vulnerabilities
- Enabling vulnerability scan:
 - Vulnerability scanning is enabled by default. You cannot disable or configure the vulnerability scan feature in FortiClient.
 - When FortiClient is in managed mode and managed by EMS, an administrator may configure and lock vulnerability scanning for you. An administrator may also disable vulnerability scanning.



FortiGate

Vulnerability name	Severity	Details
Xyz. Vulnerability	Medium	12345

<http://www.fortiguard.com/encyclopedia/vulnerability>



FORTINET

39

When endpoint users are transferring data over internet hackers can exploit vulnerabilities in endpoint devices, and use those vulnerabilities to gain unauthorized access to the system.

FortiClient can perform a vulnerability scan to search endpoint devices to identify weaknesses, provide details about the impact of those weaknesses and recommend actions to protect the applications running on the endpoint devices.

Vulnerability scanning is available on both managed and standalone clients. FortiClient communicates with the FortiGuard Center to get the signature updates.

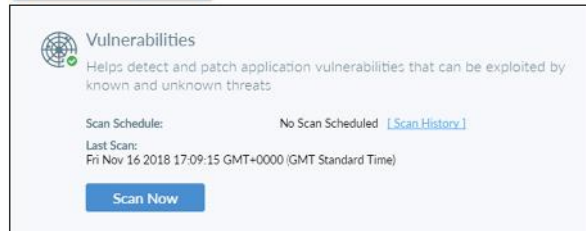
After the scan is complete, FortiClient displays the list of vulnerabilities and details. You can click on an item in the list, such as release date, severity, impact, and recommended actions, to name a few.

DO NOT REPRINT
© FORTINET

Vulnerability Management

- Compliance and vulnerability scanning
 - When FortiClient is connected to a FortiGate, FortiOS sends a FortiClient profile to FortiClient. FortiGate uses the profile to provide network security by defining compliance rules for FortiClient endpoints.
- Scan on demand
 - You can scan on demand. When the scan is complete, FortiClient displays a summary of vulnerabilities found on the endpoint. If any detected vulnerabilities require you to manually install remediation patches, the list of affected software also displays.

Vulnerability Scan



FORTINET

40

If compliance is enabled for FortiClient in managed mode, and FortiGate compliance rules require it, all automatic and manual software patches must be installed within a time frame to maintain compliant status and network access. The default time frame is one day.

However, the FortiGate administrator may choose a different time frame. Contact your system administrator to learn how long you have to fix vulnerabilities.

DO NOT REPRINT
© FORTINET

Vulnerability Management

- Automatically fixing detected vulnerabilities
 - You can automatically install software patches by clicking **Fix Now** or review detected vulnerabilities before installing software patches



- Reviewing detected vulnerabilities before fixing



FORTINET

41

Vulnerability scan identifies vulnerabilities on the endpoint that should be fixed by installing software patches. You can automatically install software patches by clicking **Fix Now** or you can review detected vulnerabilities before installing software patches. Any software patches that cannot be automatically installed are also listed and you should manually download and install software patches for the vulnerable software.

DO NOT REPRINT
© FORTINET

Vulnerability Management

- Manually fixing detected vulnerabilities
 - In some cases, FortiClient cannot automatically install software patches, and you must manually download and install software patches
- Viewing vulnerability scan history

Vulnerability Scan

Vulnerability Patch History

11/16/2018 5:09:15 PM (2)

VMware Player 12.1.1.6932 (2)

C:\Program Files (x86)\VMware\VMware Workstation\vmplayer.exe

VULNERABILITY NAME	SEVERITY	DETAILS	PATCH STATUS
VMware product updates address local privilege escalation vulnerability in linux kernel	High	≡	Unpatched
VMware Workstation and Fusion updates address out-of-bounds memory access vulnerability	High	≡	Unpatched

VMware Workstation Player 12.1.1.6932 (3)

C:\Program Files (x86)\VMware\VMware Workstation\vmplayer.exe

VULNERABILITY NAME	SEVERITY	DETAILS	PATCH STATUS
VMware Workstation update addresses multiple security issues	High	≡	Unpatched
VMware ESXi Workstation, Fusion, and Tools updates address multiple security issues	Medium	≡	Unpatched
VMware product updates address multiple important security issues	Medium	≡	Unpatched

11/14/2018 10:43:59 AM (2)

VMware Player 12.1.1.6932 (2)

C:\Program Files (x86)\VMware\VMware Workstation\vmplayer.exe

VULNERABILITY NAME	SEVERITY	DETAILS	PATCH STATUS
VMware product updates address local privilege escalation vulnerability in linux kernel	High	≡	Unpatched
VMware Workstation and Fusion updates address out-of-bounds memory access vulnerability	High	≡	Unpatched

VMware Workstation Player 12.1.1.6932 (3)

FORTINET

42

When the scan is complete, FortiClient displays a summary of vulnerabilities found on the endpoint. If any detected vulnerabilities require you to manually install remediation patches, the list of affected software also displays.

You can view the history of the last seven vulnerability scans and patches. You can view the history to see what software was identified as vulnerable and whether patches for the vulnerabilities were installed.

DO NOT REPRINT
© FORTINET

Central Management (Managed Clients Only)

- Central Management
 - Centralized client management and monitoring
 - Centralized configuration provisioning and deployment
 - Enforcement of enterprise security policies



FORTINET

43

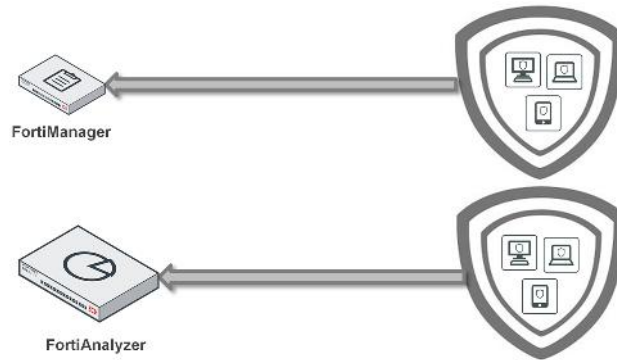
FortiClient can be fully integrated with FortiClient EMS for management and deployment. You can configure your FortiClient EMS device to discover new devices on your network, enforce FortiClient registration, and deploy FortiClient software(initial installation), and assigns FortiClient profile to connected FortiClient endpoints. The FortiClient profile can be deployed to devices on your network and over a VPN connection.

FortiGate is used for compliance enforcement. After FortiClient software is installed on endpoints, and the FortiClient endpoints connect FortiTelemetry to FortiGate, FortiClient forces the users to use the network access based on the enterprise compliance security policies configured on FortiGate. **FortiClient Compliance** security profile configured on FortiGate is used to communicate compliance rules to FortiClient endpoints.

DO NOT REPRINT
© FORTINET

Central Logging (Managed Clients Only)

- Central Logging
 - Upload logs to a FortiAnalyzer or FortiManager
 - FortiClient must be registered to FortiClient EMS to upload logs to FortiAnalyzer or FortiManager



FORTINET

44

The standalone FortiClient collects and save the logs locally, but what if logs are needed for reporting, auditing, or retention purposes?

You can register FortiClient to FortiGate or FortiClient EMS, which allows you to upload the logs to a central repository, such as FortiManager or FortiAnalyzer. From here, you can run the report or keep the logs for retention purposes.

DO NOT REPRINT
© FORTINET

Endpoint Control (Compliance and Telemetry)

- Displays whether FortiClient telemetry is connected to FortiGate or EMS
- Enforcement of up-to-date FortiClient endpoint security software on endpoints computers and mobile devices
- Pushes FortiClient profile to FortiClient application
- Forces non-compliant endpoints to install FortiClient endpoint security software

FORTINET

45

Endpoint protection enforces the use of up-to-date FortiClient endpoint security software on endpoints (workstation computers and mobile devices). FortiClient enforcement can check that the endpoint is running the most recent version of the FortiClient application, that the antivirus signatures are up-to-date, and that the firewall is enabled.

When FortiClient telemetry is connected to EMS, compliance is not enforced.

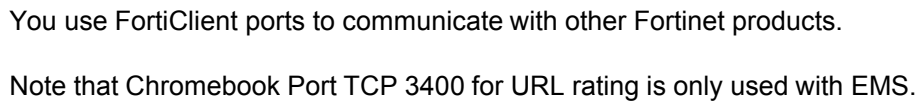
Note that you will learn more about compliance and telemetry in another lesson. This feature requires FortiOS 5.4.1 or later, or FortiClient EMS 1.0 or later.

DO NOT REPRINT
© FORTINET

Feature Support						
	WINDOWS	MAC OS X	ANDROID	iOS	ChromeBook	Linux
SECURITY FABRIC COMPONENTS						
Endpoint Telemetry ¹	✓	✓	✓	✓	✓	✓
Compliance Enforcement ¹	✓	✓	✓	✓		✓
Endpoint Audit and Remediation with Vulnerability Scanning ¹	✓	✓				✓
Automated Endpoint Quarantine	✓	✓				
HOST SECURITY AND VPN COMPONENTS						
Antivirus	✓	✓				✓
Anti-Exploit	✓					
Sandbox Detection	✓					✓
Web Filtering ²	✓	✓	✓	✓	✓	
Application Firewall ³	✓	✓				
IPSec VPN	✓	✓	✓	✓		
SSL VPN ³	✓	✓	✓	✓		✓
OTHERS						
Remote Logging and Reporting ⁴	✓	✓		✓	✓	
Windows AD SSO Agent	✓	✓				
USB Device Control	✓	✓				✓

Standalone clients support a number of features, such as VPNs, antivirus, web filtering and more. However, when a standalone client is registered with FortiGate or FortiClient EMS, it enhances comprehensive security, helping you to safeguard your systems with advanced security technologies, which are all managed from a single management console with easy provisioning, monitoring, and auditing.

You can also customize the FortiClient installation and use VPN auto-connect to ensure that FortiClient creates a VPN connection to the FortiGate when it is considered to be off-net. FortiClient also supports configuration provisioning for iOS (iOS. mobileconfig) in addition to FortiClient configuration provisioning.



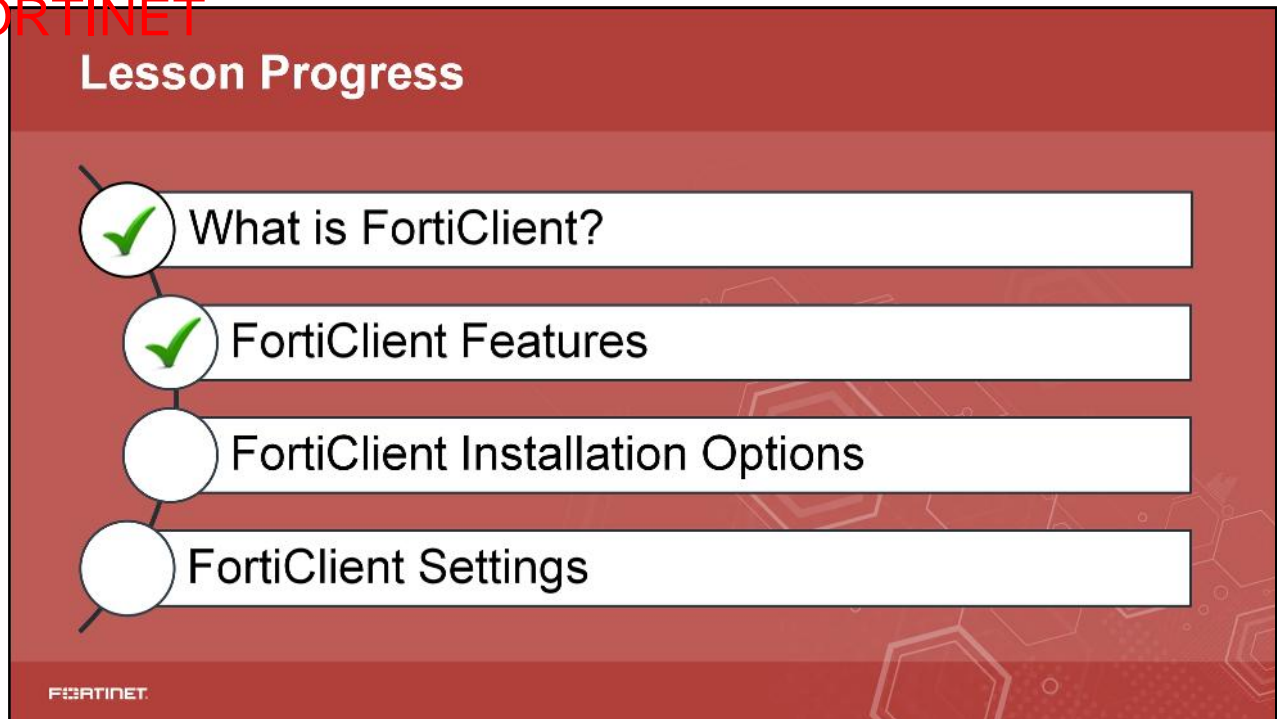
DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which of the following features are included in FortiClient malware protection?
 - A. Antivirus, vulnerability scan, and sandbox integration
 - ✓ B. Antivirus, antiexploit, and sandbox integration

2. Which VPN types are supported in FortiClient?
 - A. IPSec and PPTP
 - ✓ B. IPSec and SSL

DO NOT REPRINT
© FORTINET



Good job! You now know FortiClient features

Now, you will learn about FortiClient installation options.

FortiClient Installation

Objectives

- Identify standalone FortiClient installation options
- Identify FortiClient installation files and tools

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in identifying and understanding FortiClient installation options, tools, and features, you will be able to select the appropriate options and tools to install FortiClient in your network.

DO NOT REPRINT
© FORTINET

Standard Installation

- Standard installation
 - By default, the Secure Fabric Agent option is selected. This includes:
 - FortiClient telemetry
 - Vulnerability scanning
 - Vulnerability remediation
 - You can also select optional components, which include:
 - **Remote Access:** SSL and IPsec VPN access
 - **Advanced Persistent Threat (APT) Components:** Supports FortiSandbox
 - **Additional Security Features:** AntiVirus, Web Filtering, Application Firewall(Managed mode only), and Single Sign On
- Windows
 - FortiClientSetup_6.0.X.XXXX.exe—Standard installer for Microsoft Windows (32-bit)
 - FortiClientSetup_6.0.X.XXXX_x64.exe – Standard installer for Microsoft Windows (64-bit)
- Mac OS X
 - FortiClient_6.0.X.XX_macosx.dmg – Standard installer for Mac OS X

FORTINET

51

You can install the FortiClient as standard installation and choose the setup type that best suits your needs. For example, if you would like to install only the VPN component, you can select the **Secure Remote Access** option. If you select all options, all endpoint security and VPN components are installed.

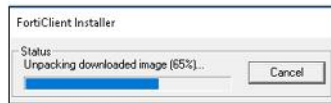
What if you want to install specific features, such as antivirus and web filtering, or you want to do VPN automation?

There are various tools and MSI package installations that you can use to configure and install a custom FortiClient installation. You will learn more about custom FortiClient installation in this lesson.

DO NOT REPRINT
© FORTINET

Standard Installation (Contd)

- Download FortiClient installation files
 - Fortinet Customer Service & Support: <https://support.fortinet.com>
 - FortiClient homepage: www.forticlient.com
 - You always get the latest release
- Using the FortiClient online installer is recommended:
 - Launches FortiClient virus cleaner prior to installing FortiClient



- Allows you to select features to be installed



FORTINET

62

You can download the FortiClient installation file from the Fortinet support site or the FortiClient home page. The FortiClient home page will always have latest release of FortiClient. If you need an older version of FortiClient, use Fortinet service and support website.

When you install FortiClient, you can select which setup type and options to install:

- **Security Fabric Agent:** Selected by default. This option installs components to support the security fabric available with FortiGate, including FortiClient telemetry, vulnerability scanning, and vulnerability remediation.
- **Secure Remote Access:** Optional. This option supports SSL and IPsec VPN access.
- **Advanced Persistent Threat (APT) Components:** Optional. Supports FortiSandbox.
- **Additional Security Features:** Optional. This option supports antivirus, web filtering, application firewall, and single sign-on. You can select one, several, or all security options.

DO NOT REPRINT
© FORTINET

MSI Package Installation

- FortiClientSetup_6.0.X.XXXX.zip–FortiClient.msi and language transforms for Microsoft Windows (32-bit)
- FortiClientSetup_6.0.X.XXXX_x64.zip–FortiClient.msi and language transforms for Microsoft Windows (64-bit)
- MSI installer packages can be created using FortiClient configurator tool
 - Can be deployed using Microsoft Active Directory (AD) server or Microsoft SCCM 2012 or any other delivery tool that can deploy MSI can be used

FORTINET

53

MSI installers are supported in Microsoft Windows environments only.

`FortiClientSetup_6.0.X.XXXX.zip`: A zip package containing `FortiClient.msi` and language transforms for 32-bit Windows. Some properties of the MSI package can be customized with `FortiClientConfigurator.exe`, which can be found in `FortiClientTools_6.0.X.XXXX.zip`.

`FortiClientSetup_6.0.X.XXXX_x64.zip`: A zip package containing `FortiClient.msi` and language transforms for 64-bit Windows. Some properties of the MSI package can be customized with `FortiClientConfigurator.exe`, which can be found in `FortiClientTools_6.0.X.XXXX_x64.zip`.

The MSI installer in the .zip file package is customizable for a larger roll out to many computers in an organization.

DO NOT REPRINT
© FORTINET

FortiClient Tools

- FortiClient tools
 - A package containing miscellaneous tools including the FortiClient VPN automation files
 - Allows you to choose to which features to install
 - Can select to enable or disable software updates, and configure SSO
- FortiClientTools_6.0.X.XXXX.zip for windows contains:
 - FortiClientVirusCleaner
 - OnlineInstaller
 - SupportUtils
 - VPNAutomation
 - SSLVPNcmdline
- FortiClientConfigurationTool_6.0.X.XXX.zip
 - FortiClientConfigurator.exe
- FortiClientTools_6.0.X.XX_macosx.tar for Mac OS contains:
 - OnlineInstaller
 - FortiClientConfigurator

FORTINET

54

The FortiClient tools package contains various tools you can use to customize your FortiClient installation. These tools include:

- **FortiClientVirusCleaner:** This tool was developed to identify and cleanse systems of viruses.
- **OnlineInstaller:** FortiClientInstaller.exe downloads and installs the latest FortiClient from public FDS.
- **SupportUtils:** Contains various miscellaneous tools:
 - **RemoveFCTID.exe:** A tool to remove the unique identifier
 - **FCRemove.exe:** A clean up tool for use only if the **Add/Remove Programs** applet fails to remove FortiClient
 - **ReinstallNIC.exe:** A tool for use on Windows7 if DHCP address allocation is slow
 - **FortiClient_Diagnostic_Tool.exe:** A tool to gather information, such as FortiClient connection to FortiGuard Distribution Server (FDS), general system information, and installed features information, all of which can be useful for troubleshooting
- **VPNAutomation:** FCCOMIntDLL.tlb is a typeog library needed for building applications that use FortiClient's IPsec VPN COM interface.
- **SSLVPNcmdline:** FortiSSLVPNClient.exe is a command line tool for controlling SSL-VPN tunnels.

FortiClientConfigurationTool:

- **FortiClientConfigurationTool.exe:** FortiClient MSI files can be configured.

Mac OS X FortiClient tools file contains the following:

- **OnlineInstaller:** Downloads and installs the latest FortiClient file from the public FDS
- **FortiClientConfigurator:** An installer repackaging tool that can be used to create custom installation packages.

Note that starting with version 5.6, FortiClient Configurator is available without a license on the Fortinet Developer Network (<https://fndn.fortinet.net>).

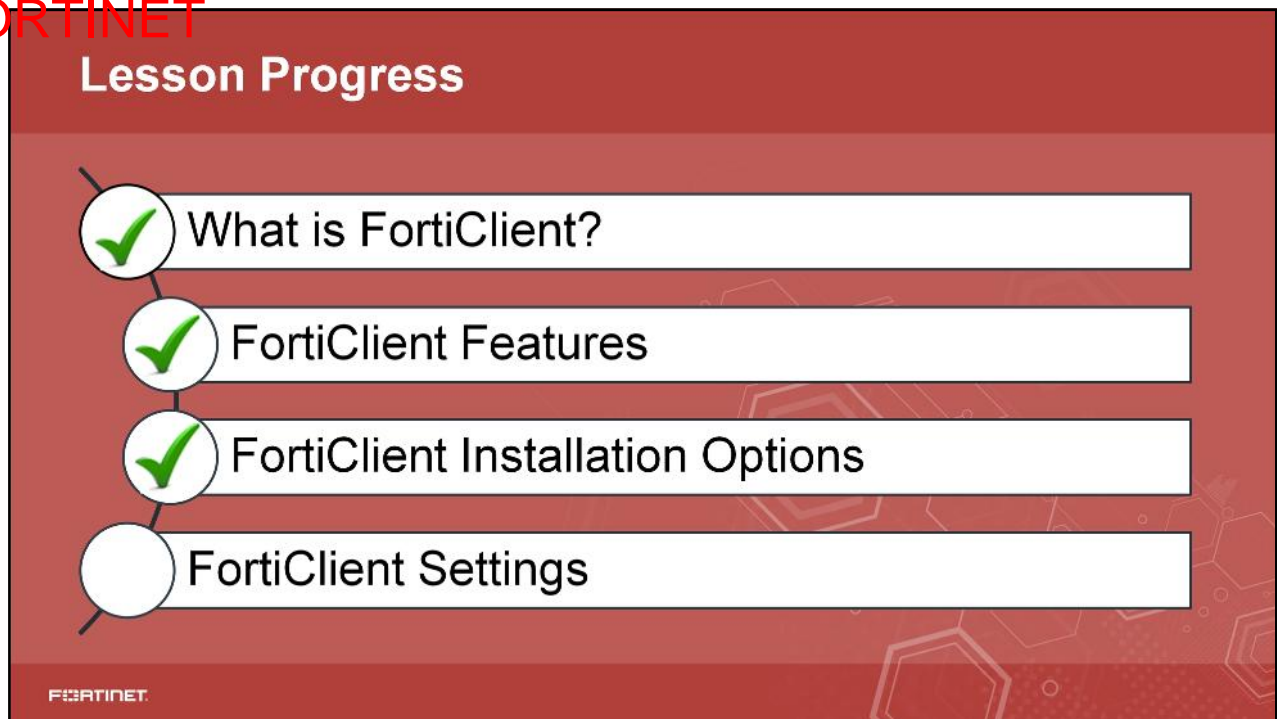
DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which FortiClient component is selected by default and cannot be removed?
 - A. Advanced persistent threat
 - ✓ B. Security fabric agent

2. Which installation package can you use to install a custom FortiClient?
 - ✓ A. MSI package
 - B. Online installer

DO NOT REPRINT
© FORTINET



Good job! You now know FortiClient Standalone installation

Now, you will learn about FortiClient general settings.

DO NOT REPRINT
© FORTINET

FortiClient Settings

Objectives

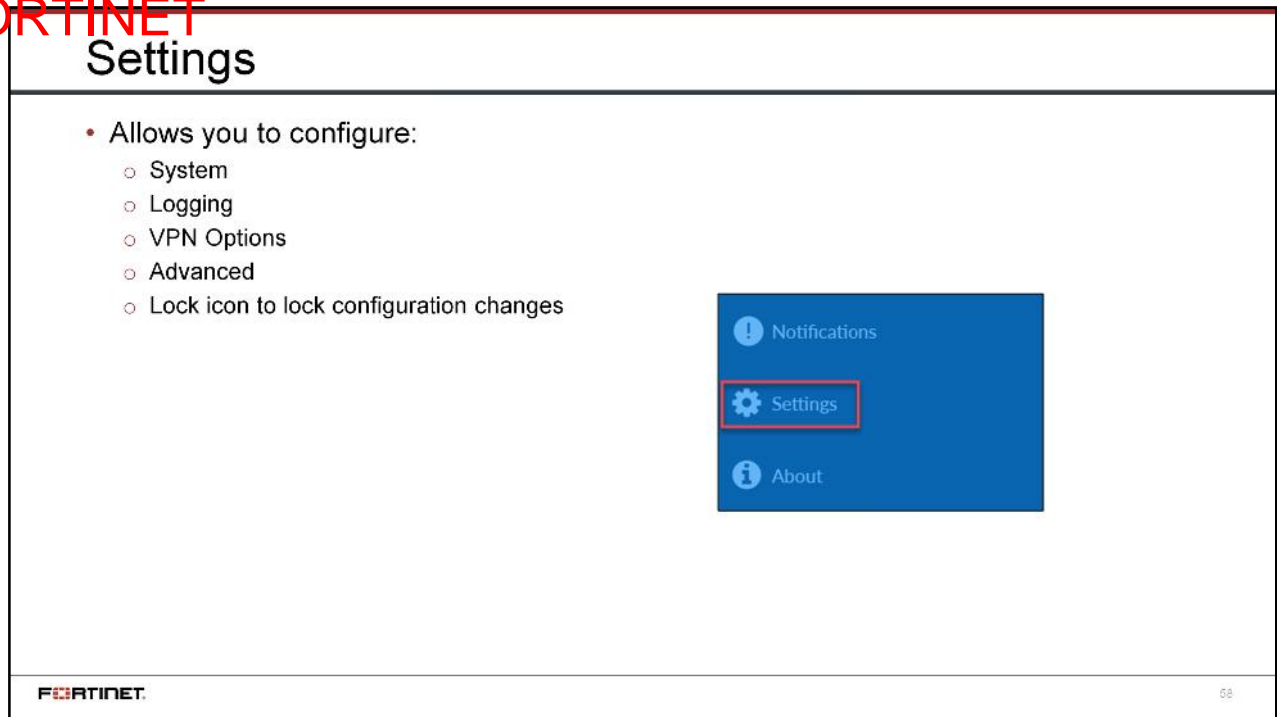
- Identify FortiClient settings

FORTINET

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding FortiClient settings, you will be able to use them effectively when setting up FortiClient.

DO NOT REPRINT
© FORTINET



The additional settings that are available on the FortiClient when you click **Settings**, allow you to configure:

- System
- Logging
- VPN options
- Advanced
- Lock icon to lock configuration changes

You will be exploring and configuring these options in detail in this lesson.

DO NOT REPRINT
© FORTINET

Settings—System

- Allows you to configure
 - System
 - Backup or restore options
 - Software update options

Settings > System

System

Backup or restore full configuration Backup Restore

Software update

☐ Automatically download and install updates

☒ Alert when updates are available

Settings > System

System

Backup or restore full configuration Backup Restore

File

Password

Re-enter Password

Backup Comments

☐

Software update

☐ Automatically download and install updates

☒ Alert when updates are available

Sample partial backup

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
  <forticlient_version>6.0</forticlient_version>
  <version>6.0.3</version>
  <exported_by_version>6.0</exported_by_version>
  <date></date>
  <partial_configuration>0</partial_configuration>
  <os_version>windows</os_version>
  <os_architecture>x64</os_architecture>
  <system>
    <ui>
      <disable_backup>0</disable_backup>
      <ads>1</ads>
    </ui>
  </system>
</forticlient_configuration>
```

There are additional settings available on the FortiClient *Settings*, which includes:

The **System** menu allows you to:

- Backup:** You can backup FortiClient configuration in standalone mode or when registered to FortiGate or EMS.
- Restore:** You can restore FortiClient configuration **only** in standalone mode.

Note that the FortiClient configuration file is XML format configuration file. When performing a backup, you can select the file destination and save the file in an unencrypted (.conf) or encrypted format (.sconf). You include or exclude comments in the XML configuration file.

- Software Updates:** You can configure the behavior of FortiClient when a new software version is available on the FDS and can be configured only when in standalone mode, in the managed mode this setting is pushed by EMS.

DO NOT REPRINT
© FORTINET

Settings—Logging, VPN

- Allows you to configure
 - Logging
 - Enable logging for features
 - Specify log level
 - Export and clear logs
 - VPN Options
 - **Enable VPN before logon**
 - **Preferred DTLS Tunnel**

Settings > Logging

— Logging

Enable logging for these features:

<input checked="" type="checkbox"/> VPN	<input checked="" type="checkbox"/> Telemetry
<input checked="" type="checkbox"/> Antivirus	<input checked="" type="checkbox"/> Web Security
<input checked="" type="checkbox"/> Update	<input checked="" type="checkbox"/> Vulnerability Scan
<input checked="" type="checkbox"/> Sandboxing	

Log Level: Information ▼

Log file: Export logs Clear logs

Settings > VPN Options

— VPN Options

☐ Enable VPN before logon

☐ Preferred DTLS Tunnel

The **Logging** menu allows you to enable and disable logging for features (VPN, antivirus, web security, and update), specify log level, export logs, and clear logs. By default, logging for VPN, antivirus, web Security, telemetry, vulnerability scan, sandboxing and update is enabled. The default log level is **Information**.

Did you notice there is no option for logging for application firewall? Why?

This is because these features are available only to registered clients, and because logging can be enabled from only a management console, such as FortiClientEMS.

The **VPN Options** dropdown menu makes the **Enable VPN before logon** option available. This requires that the Windows log on screen is not bypassed. On the Microsoft Windows side, you also need to enable the User must enter a user name and password on this computer option in the User Accounts settings. You can prefer DTLS over TLS by selecting **Preferred DTLS Tunnel**.

Note that DTLS over TLS setting is only available for Windows endpoint.

DO NOT REPRINT
© FORTINET

Settings—Advanced

- Allows you to configure
 - Default tab
 - Advanced
 - Enable Single Sign-On mobility agent
 - Disable proxy (troubleshooting only)



FORTINET

61

The **Advanced** menu allows you to enable:

- **Default tab:** You can select the default tab to display on FortiClient while on the launch console.
- **Single Sign-On mobility agent:** It allows you to configure single sign-on (SSO) mobility agent for FortiAuthenticator. You must apply a FortiClient SSO mobility agent license to your FortiAuthenticator device. The default port is set to 8001. The FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. The FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgement packet. FortiClient to FortiAuthenticator communication requires the following:
 - The IP address should be unique in the entire network.
 - The FortiAuthenticator should be accessible from clients in all locations.
 - The FortiAuthenticator should be accessible by all FortiGates.

Note that FortiClient SSO mobility agent requires a FortiAuthenticator running v2.0.0 or later, or v3.0.0 or later.

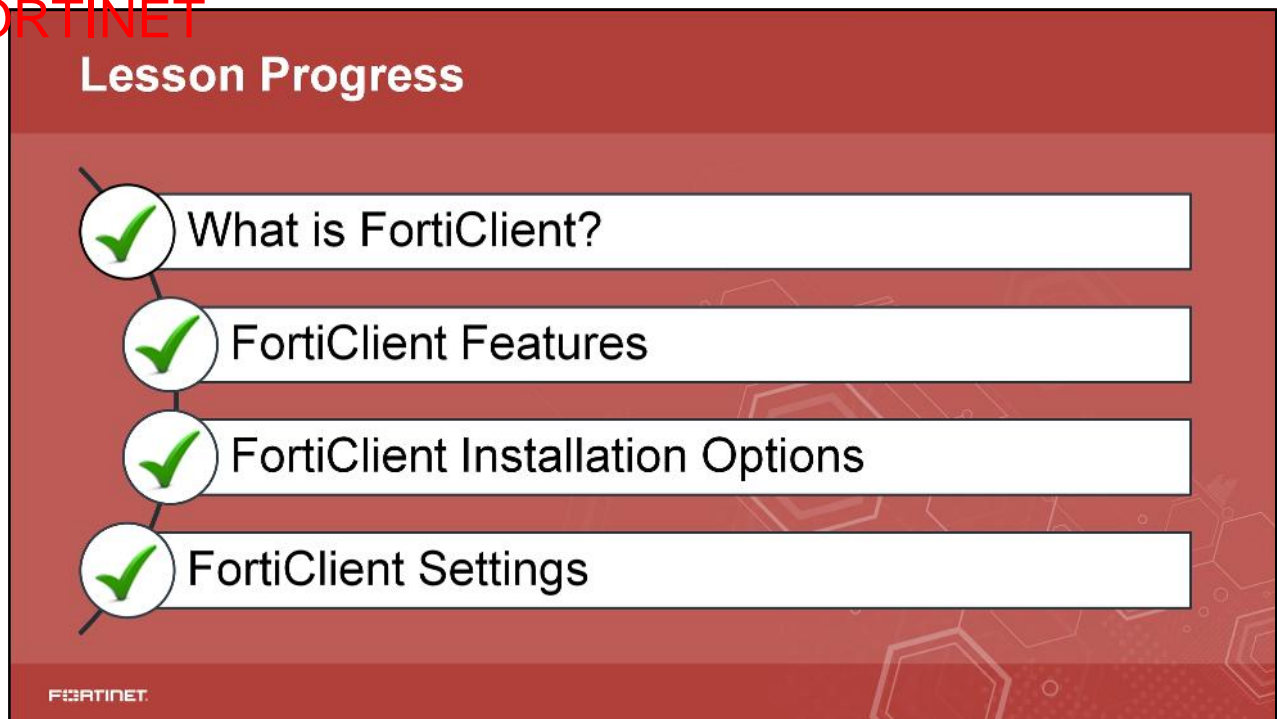
DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which of the following is the default log level configured on FortiClient?
 - A. Critical
 - ✓ B. Information

2. Which of the following components does FortiClient single sign-on mobility require?
 - ✓ A. FortiAuthenticator
 - B. FortiClientEMS

DO NOT REPRINT
© FORTINET



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

DO NOT REPRINT
© FORTINET

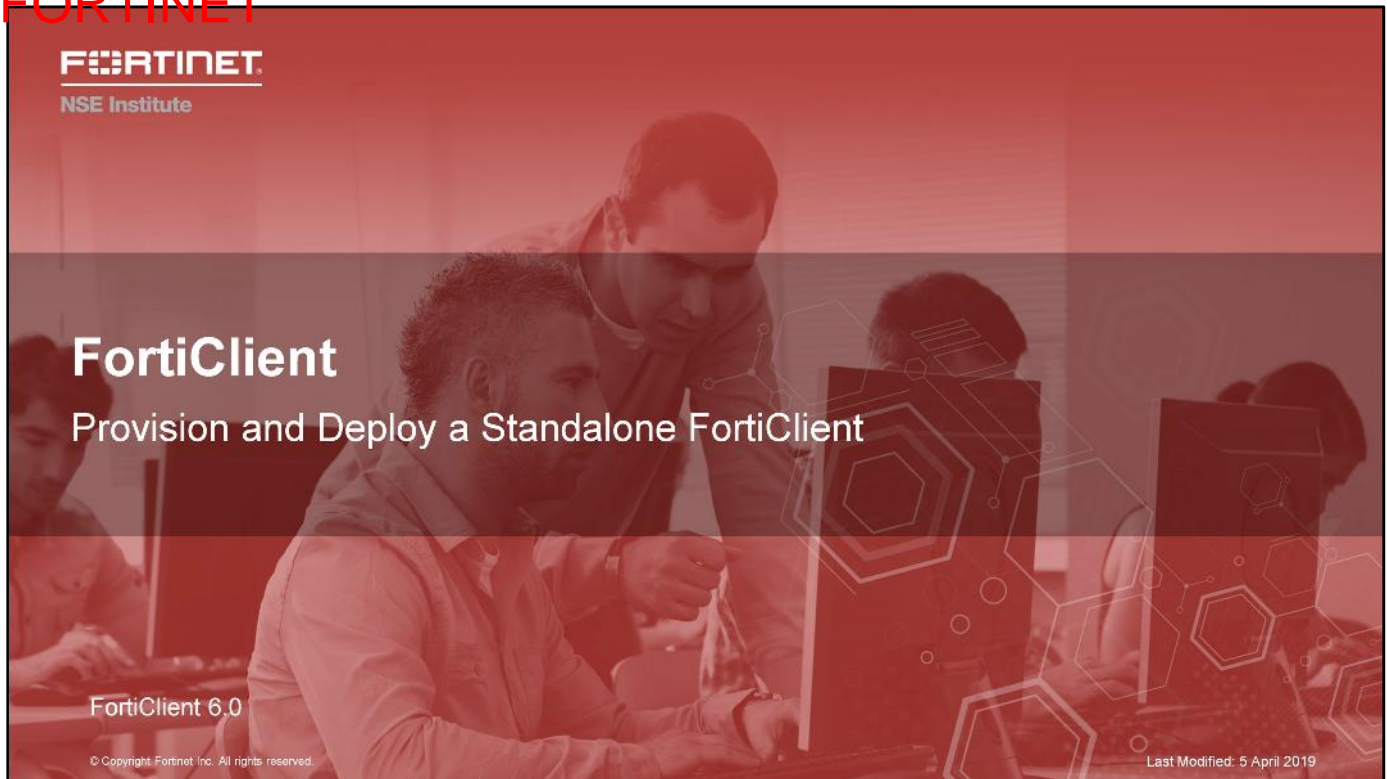
Review

- ✓ Know when and why FortiClient endpoint security
- ✓ Identify endpoint security features
- ✓ Identify FortiClient modes
- ✓ Identify FortiClient key features
- ✓ Identify FortiClient standalone client features and managed client features
- ✓ Identify standalone FortiClient installation options
- ✓ Identify FortiClient installation files and tools
- ✓ Identify FortiClient settings

FORTINET

This slide shows the objectives covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FortiClient features and options to install and use FortiClient to secure endpoints in your network.



In this lesson, you will learn how to provision and deploy a standalone FortiClient in your existing network, to manage the security of multiple endpoints.

Lesson Overview

- 1 Identify Methods of Provisioning a Standalone FortiClient
- 2 Understand and Configure FortiClient XML
- 3 Create Custom FortiClient Installation Packages
- 4 Identify Methods of Deploying FortiClient
- 5 Uninstall FortiClient

FORTINET

In this lesson, you will learn about the topics shown on this slide.

Provisioning a Standalone FortiClient

Objectives

- Identify methods of provisioning FortiClient

FORTINET

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in provisioning a standalone FortiClient, you will be able to provision FortiClient in your network.

DO NOT REPRINT
© FORTINET

Provisioning FortiClient

- Various methods to provision FortiClient
- Allows you to choose which features you want to install
- Multiple methods to create custom installation files
 - FortiClient Configurator Tool
 - FortiClient Enterprise Management Server (EMS)
- Custom installation further allows granular selection of features to install

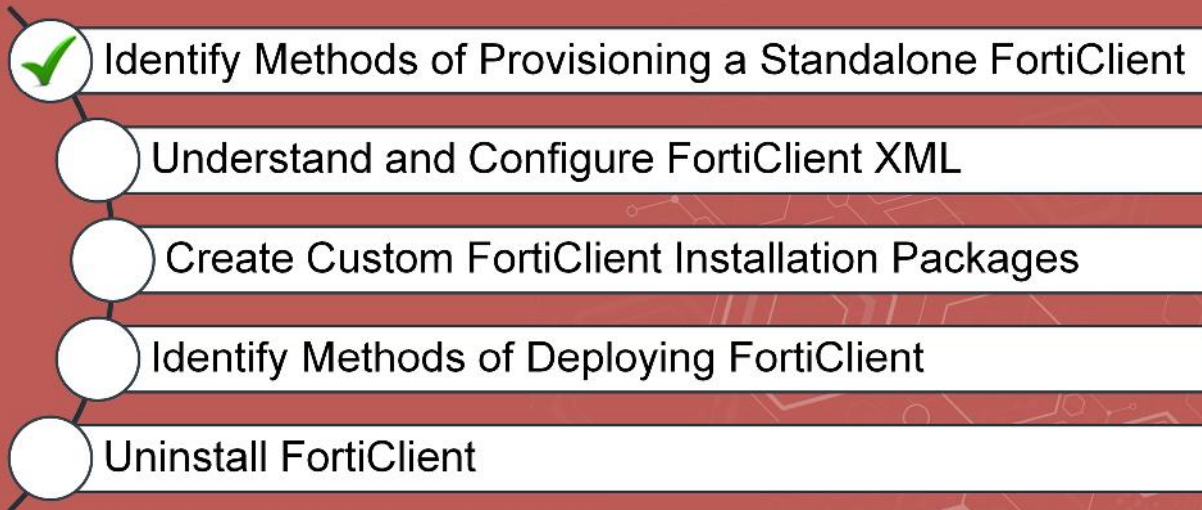
You can use the following methods to provision FortiClients.

- **FortiClient Configurator Tool:** Use to configure FortiClient MSI files.
- **FortiClient Enterprise Management Server:** Use to provision, deploy, and manage endpoints. You will learn about this method later in this lesson.

You can also customize FortiClient installation features using these tools. These tools also allow you to select specific FortiClient features.

Note that the MSI Editor is third-party tool and is not covered in this course.

Lesson Overview

- 
- ✓ Identify Methods of Provisioning a Standalone FortiClient
 - Understand and Configure FortiClient XML
 - Create Custom FortiClient Installation Packages
 - Identify Methods of Deploying FortiClient
 - Uninstall FortiClient

FORTINET

Good job! You now understand how to provision FortiClient.

Now, you will learn how to configure FortiClient XML.

Configuring FortiClient XML

Objectives

- Understand FortiClient XML settings
- Configure FortiClient XML settings

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring FortiClient XML, you will be able to configure FortiClient XML settings.

DO NOT REPRINT
© FORTINET

FortiClient XML Configuration

- Extensible Markup Language (XML)
 - Set of rules in a format for encoding documents
 - Both human readable and machine-readable
- Import and export FortiClient configurations via XML file
- File extensions
 - .conf
 - .sconf
- Configuration file generated from
 - FortiClient: **File** > **Settings** > **System**
 - `FCConfig.exe`: Command line program installed with FortiClient

XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

FortiClient supports importation and exportation of its configuration in an XML file, and supports two file types, which are:

- **.conf**: A plain-text configuration file.
- **.sconf**: A secure (encrypted) configuration file

You can generate and back up a configuration file (which is an XML file) on the **Settings** page of the FortiClient dashboard, or by using the command-line program `FCConfig.exe`, which is installed with FortiClient.

DO NOT REPRINT
© FORTINET

XML Configuration—File Section

- The XML configuration file contains
 - Metadata
 - System settings
 - Endpoint control
 - VPN
 - Certificates
 - Antivirus
 - Single sign-on mobility agent
 - Web Filtering
 - Application firewall
 - Vulnerability scan
- Boolean values
 - 0 means false (feature is disabled)
 - 1 means true (feature is enabled)

FORTINET

8

For the purpose of understanding the FortiClient XML configuration, the major sections of the XML configuration are as follows:

- **Metadata:** Facilitates the discovery of relevant information and is basic data controlling the entire configuration file.
- **System settings:** General settings that are not specific to any of the modules listed below (or affect more than one module)
- **Endpoint control:** Includes settings related to controlling endpoints, such as enable enforcement, off-net update, skip confirmation, disable unregister, silent registration, and so on.
- **VPN:** Includes settings related to global options that apply to both SSL VPN and IPsec VPN, and settings related to SSL VPN and IPsec VPN individually.

You can also configure XML for settings related to certificates, antivirus, single sign-on mobility agent, web filtering, application firewall, and vulnerability scan.

The XML configuration is controlled by two boolean values (usually denoted true and false) that enable or disable a configuration setting:

- 0 means false (feature is disabled)
- 1 means true (feature is enabled)

Also in this lesson, you will learn how to enable and disable specific configuration settings.

XML Configuration—Metadata

- Configuration file is contained inside XML tag
- `<forticlient_configuration>`
- Standard XML start tag which includes XML version number and encoding
- `<?xml version="1.0" encoding="utf-8"?>`
- Empty configuration will look like the following example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
</forticlient_configuration>
```

Start of FortiClient configuration

End of FortiClient configuration

- Sample meta data

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
  <forticlient_version>6.0.x.xxx</forticlient_version>
  <version>6.0.x</version>
  <exported_by_version>6.0.x.xxx</exported_by_version>
  <date>2019/xx/xx</date>
  <partial_configuration>0</partial_configuration>
  <os_version>Windows</os_version>
```

FortiClient version

Date of configuration generated

0→Config will be replaced
1→Config will be added

OS version – Windows or Mac OS X

All of the XML tags and data in a configuration file are contained inside the XML tag `<forticlient_configuration>`. The first line of the configuration starts with a standard XML start tag `<?xml version="1.0" encoding="utf-8"?>` which includes the XML version and encoding.

The XML configuration has elements (or nested child elements) that begin with a start tag and end with a matching end tag. An empty FortiClient configuration would look like the following:

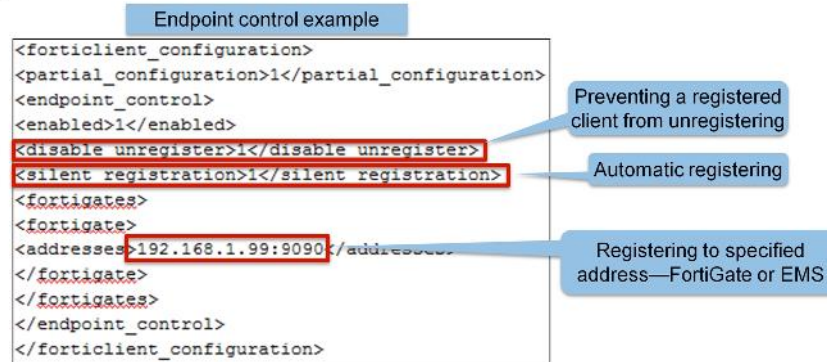
```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>    → Start tag
</forticlient_configuration> → Matching end-tag
```

If you export the configuration from FortiClient, it will include the FortiClient version, date of generation, and OS version (Windows or Mac OS X) from where the configuration was generated; either FortiGate or FortiClient EMS.

`<partial_configuration> 0 or 1 </partial_configuration>` is a line of metadata that controls whether the configuration will be replaced or added in an import or restore. The value 0 will replace the configuration and the value 1 will append the configuration to the existing configuration.

XML Configuration—Endpoint Control

- Endpoint control configuration usually downloaded from FortiGate or EMS
- Divided into two sections
 - Endpoint control general attributes
 - Specific feature configurations



The endpoint control configuration element controls settings related to controlling endpoints such as disable unregister, silent registration, enable enforcement, off-net update, skip confirmation, and which features to display on the FortiClient console, and so on.

You usually download the endpoint control configurations from the FortiGate or EMS or you can build it using the *XML Reference Guide* available at <http://docs.fortinet.com> in the FortiClient XML configuration section.

The endpoint control configurations are divided into two parts:

- Endpoint control general attributes: These are contained in the `<endpoint_control></endpoint_control>` XML tags.
- Configuration details relating to specific FortiClient services, such as antivirus, web filtering, application firewall, vulnerability scanner, and so on, are found in their respective configuration elements contained inside their XML tags. For example, the antivirus configuration is contained in the `<antivirus></antivirus>` XML tags.

In the example shown on this slide `silent_registration`, which allows you to automatically register on FortiGate or FortiClient EMS without prompting the user to accept the registration. Silent registration is intended to be used with `disable_unregister`, which prevents a registered client from being able to unregister after successfully registering on a FortiGate or FortiClient EMS server.

The `addresses` XML setting defines that FortiClient will attempt to register on the first FortiGate or EMS listed here. You can add multiple IP's delimited with a semicolon.

XML Design Considerations

- FortiClient configuration file is user editable
 - Uses XML format for easy parsing and validation
- Design considerations
 - Input validation
 - Handling of password fields
 - Segment of configuration file
 - Client certificate

Valid segment of configuration file

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
  <system>
    <remote_logging>
      <log_upload_enabled>1</log_upload_enabled>
      <log_upload_server>10.0.1.210</log_upload_server>
    </remote_logging>
  </system>
</forticlient_configuration>
```

Invalid segment of configuration file

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
  <remote_logging>
    <log_upload_enabled>1</log_upload_enabled>
    <log_upload_server>10.0.1.210</log_upload_server>
  </remote_logging>
</forticlient_configuration>
```

Does not follow syntax and hierarchy level.
Missing <system> syntax and hierarchy level.

The FortiClient configuration file is user editable and includes all client configurations. When building an XML configuration, you should adopt the following design considerations:

- **Input validation:** The import function performs basic validation, and writes to a log when errors or warnings are found. The default values for omitted configurations are ignored, but for VPN they are defined in the configuration.
- **Handling of password fields:** The password and username fields will be encrypted (prefixed with "Enc") when a configuration is exported; however, the import function is able to take either the clear text or encrypted format.
- **Segment of configuration file:** The XML configuration allows you to import the segment (partial configuration) of a configuration file; however, the segment should follow the syntax and hierarchy defined in the *XML Reference Guide* available at <http://docs.fortinet.com>.

In the example, invalid segment configuration file is missing the hierarchy and syntax for <system> level commands and is considered to be an invalid segment.

- **Client certificate:** The client certificate(s) are exported in an encrypted format in the configuration file.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. In XML, feature configuration is controlled by?
 - A. Decimal value
 - ✓ B. Boolean value

2. Which two parts make up the endpoint control configuration?
 - ✓ A. Endpoint control general attributes and specific feature configurations
 - B. Metadata and system settings

Lesson Overview

- ✓ Identify Methods of Provisioning a Standalone FortiClient
- ✓ Understand and Configure FortiClient XML
- Create Custom FortiClient Installation Packages
- Identify Method of Deploying FortiClient
- Uninstall FortiClient

FORTINET

Good job! You now understand how to configure FortiClient XML.

Now, you will learn how to use FortiClient Configurator Tool to create custom installation packages.

Creating custom FortiClient Installation Packages

Objectives

- Create custom installation packages using FortiClient Configurator Tool

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in creating custom FortiClient installation packages, you will be able to create and configure installation packages using FortiClient Configurator Tool.

FortiClient Configurator Tool

- Starting with FortiClient 5.6.0, FortiClient Configurator Tool is free; no license key is required to use the tool
- FortiClient Configurator Tool is available for both Microsoft Windows and Mac OS X operating systems
- To download the tool
 - 1. Log in to your FNDN account at <https://fndn.fortinet.net/>
 - 2. Click **Tools** > **Personal Toolkit**, and download FortiClient Configurator Tool
- Allows you to create customized installer packages to:
 - Include which features to install
 - Enable software updates
 - Include custom FortiClient XML configuration file
 - Add gateway IP list
 - Create desktop shortcut
 - Add FortiClient to startup menu

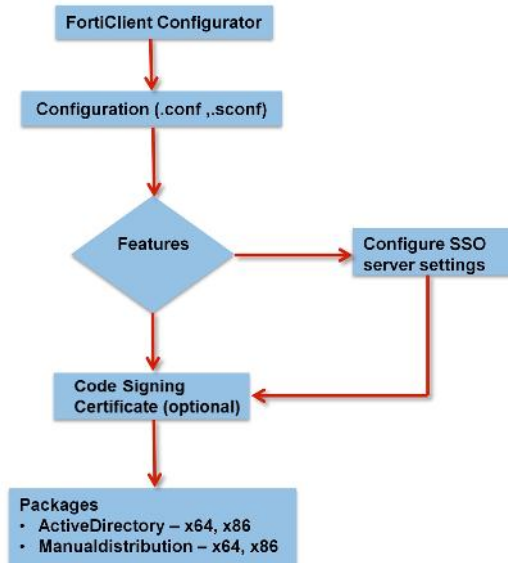
The following steps provide an overview of how you use the FortiClient Configurator Tool:

1. Log in to your FNDN account, and download the tool from FNDN.
 - If you do not have an account for FNDN, you must create an account at <https://fndn.fortinet.net/index.php?/register/>. When you create an FNDN account, you are required to include the email address of two Fortinet sponsors. Fortinet sponsors are Fortinet employees who can verify that you are a Fortinet customer. Contact your sales representative or sales engineer for the email addresses of Fortinet sponsors.
2. You have the option to add a FortiClient configuration file and/or a telemetry gateway IP list to the FortiClient installer. Before you create the installer, you should get these files ready for selection.
3. Create a custom FortiClient installer.
4. Deploy the custom FortiClient installation packages.

DO NOT REPRINT
© FORTINET

Creating a Custom Installer Package

- Flowchart



FORTINET

16

This flowchart on this slide shows the process to create a custom FortiClient installer package using FortiClient Configurator Tool.

As you can see, FortiClient Configurator Tool allows you to select an XML configuration file, select features and options, and create packages for Active Directory and manual distribution for both x64 and x86 system versions.

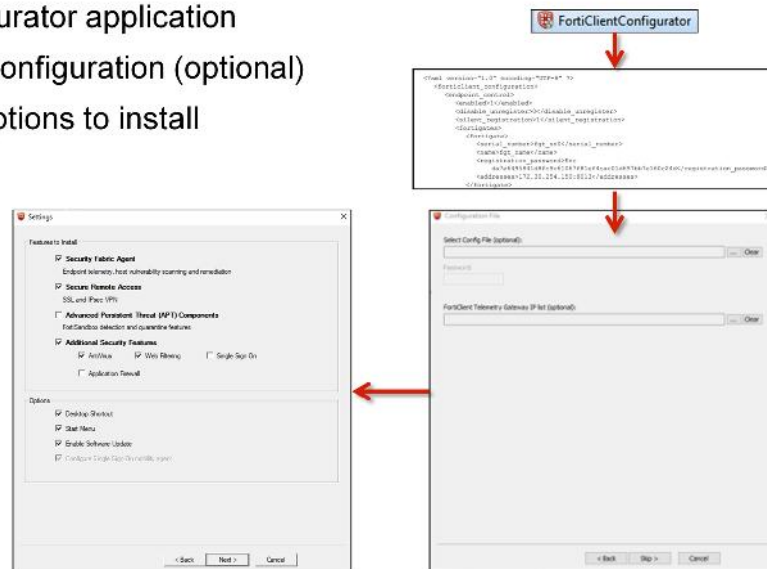
When you select custom features to install, only the modules you select are installed. To enable other features, you will need to uninstall FortiClient, and reinstall an MSI file with these features, included in the installer.

As a general recommendation, it is good to install all features and activate only the modules which are required. Doing this gives you the flexibility to enable unused features in the future.

Note that FortiClient 6.0 was introduced with a new GUI and no longer supports the rebranding tool.

Customize Using FortiClient Configurator Tool

- Run FortiClientConfigurator application
- Upload custom XML configuration (optional)
- Select features and options to install



FORTINET

17

The following are the steps involved in creating a custom installer package using FortiClient Configurator Tool:

1. Run the FortiClient-Configurator application.
2. Optionally, add a configuration file (.conf, .sconf), which will be included in the installer file.
3. Select the features you want to install:
 - **Security Fabric Agent:** Endpoint telemetry, host vulnerability scanning, and remediation. By default, selected to support Fortinet Security Fabric.
 - **Secure Remote Access:** Only SSL and IPSec VPN will be installed.
 - **Advanced Persistent Threat:** FortiSandbox detection and quarantine features will be installed.
 - **Additional Security Features:** You can select one of the following:
 - **AntiVirus**
 - **Web Filtering**
 - **Application Firewall**
 - **Single SignOn**
 - Options such as **Desktop shortcut**, **add FortiClient to start menu**, and **enable software updates**.

Customize Using FortiClient Configurator Tool

- SSO server settings

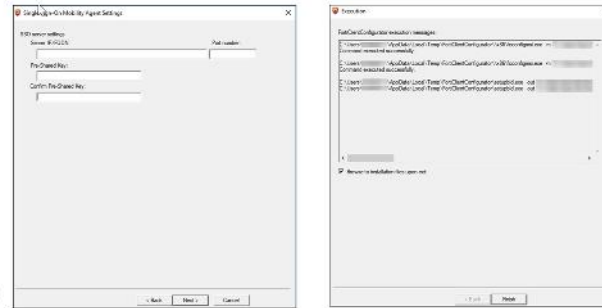
- Server IP address
- Port number
- Pre-shared key

- Select code signing certificate (optional)

- Select the code signing certificate on your management computer

- Creates packages for

- Active Directory: x86, x64
- Manual distribution: x86, x64



Name	Date modified	Type
x64	08/01/2019 10:01	File folder
x86	08/01/2019 10:01	File folder

Name	Date modified	Type
ActiveDirectory	08/01/2019 10:01	File folder
ManualDistribution	08/01/2019 10:01	File folder

You can also select SSO server settings if you need to install an SSO agent.

If you have a code signing certificate, you can use it to digitally sign the installer package FortiClient Configurator Tool generates. If you do not want to digitally sign the installer package, select **Skip** to continue.

Finally, clicking on finish will create a custom installer package for both manual distribution and Active Directory for Windows (x64 and x86). The file location will be:

C:\Users\Fortinet\Downloads\FortiClientConfigurationTool_6.0.X.XXX\repackaged\6.0.X.XX
X-EPC-VULN-VPN-AV-WF_<Date>.

FortiClient Configurator Tool creates files for both 32-bit (x86) and 64-bit (x64) operating systems. Before deploying the custom MSI files, you should test the packages to confirm that they install correctly. An .exe installation file is created for manual distribution.

FortiClient Configurator Tool for Mac OS X

- To create a custom FortiClient installation file:
 - Click the `FortiClient Configurator.dmg` application file, and double-click the **FCTConfigurator** icon to launch the tool
 - Configure the following settings, and click **Next**:
 - Source
 - Destination
 - Customize installer
 - Upload a configuration file (optional), or select a FortiClient configuration file (.conf, .sconf) to include in the installer file
 - Select **IP List File**(Telemetry Gateway IP)
 - Features to install
 - Select features and options you want to install
 - Click **Done** to deploy repackaged FortiClient

The steps are similar to a Windows custom installation package, except for a few settings.

- **Source:** Select the FortiClient installer file on your management computer. You must use the full installer file; otherwise, FortiClient Configurator Tool will fail to create a custom installation file. The FortiClient installer version and FortiClient Configurator Tool version must match; otherwise, FortiClient Configurator Tool will fail to create a custom installation file.
 - **Destination:** Enter a name for the custom installation file and select a location to save the file to your management computer.
 - Features include:
 - **Security Fabric Agent:** Endpoint telemetry, host vulnerability scanning, and remediation. By default selected to support the Fortinet Security Fabric.
 - **Secure Remote Access:** Only SSL and IPSec VPN will be installed.
 - **Advanced Persistent Threat:** FortiSandbox detection and quarantine features will be installed.
 - **Additional Security Features:** You can select one of the following in the drop-down list:
 - **AntiVirus**
 - **Web Filtering**
 - **Application Firewall**
 - **Single SignOn**
 - You can select options such as **Single Sign-On** mobility agent and **enable software updates**.
- For Mac OS, FortiClient Configurator Tool will generate the `.dmg` file.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. FortiClient Configurator Tool creates which Windows OS file(s)?

- A. .dmg
- ✓ B. Both 32-bit and 64-bit

2. Which file is used for manual distribution?

- A. .msi
- ✓ B. .exe

Lesson Overview

- ✓ Identify Methods of Provisioning a Standalone FortiClient
- ✓ Understand and Configure FortiClient XML
- ✓ Create Custom FortiClient Installation Packages
- Identify Methods of Deploying FortiClient
- Uninstall FortiClient

FORTINET

Good job! You now understand how to use the FortiClient Configurator Tool to create custom installation packages.

Now, you will learn about methods of deploying FortiClient.

Deploying FortiClient

Objectives

- Identify methods of deploying FortiClient

FORTINET

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in deploying FortiClient, you will be able to use different methods of deploying FortiClient.

FortiClient Installation Using Microsoft AD Server

- Can deploy FortiClient using Microsoft Active Directory (AD) server
- General steps to deploy:
 - Create a distribution point
 - Create a shared network folder and set permissions to allow access to distribution package
 - Copy FortiClient MSI installer package
 - Copy FortiClient MST package
 - Create a Group Policy Object
 - Select groups you would like to install FortiClient
 - Assign the package
 - Assign package by selecting the path of your distribution point and FortiClient installer file
 - FortiClient will be installed on next client computer reboot

You can also deploy FortiClient to endpoints using a Microsoft AD server. The general steps to deploy FortiClient using a Microsoft AD server are as follows:

- Create a distribution point
- Create Group Policy
- Assign the package

Note that these steps may vary based on your version of Microsoft server, Microsoft Management Console (MMC), or snap-in location.

TIP: If you want to expedite the installation process, you can force a Group Policy Object (GPO) update.

FortiClient Installation via Microsoft SCCM (2012)

- Can deploy FortiClient using Microsoft System Center Configuration Manager 2012 (SCCM)
- General steps to deploy:
 - Map the network drive where FortiClient MSI is saved
 - Create new custom task sequence
 - Define the path, drive, and account allowed to access it
 - Create a new task sequence
 - Copy FortiClient MSI image from network shared directory
`cmd /c copy /y G:\FortiClient.msi c:\temp\FortiClient.msi`
 - Copy FortiClient MST image from network shared directory
`cmd /c copy /y G:\FortiClient.mst c:\temp\FortiClient.mst`
 - Install FortiClient using MSI image
`cmd /c msixexec /i c:\temp\FortiClient.msi /qn TRANSFORMS=FortiClient.mst`
 - Deploy the task sequence
 - Select the client collection to which this task sequence should be deployed
 - Select the deployment settings

You can also deploy and manage multiple FortiClient installations using the SCCM. The general steps to deploy FortiClient using the Microsoft System Center 2012 Configuration Manager (SCCM) are as follows:

- Map the network drive where FortiClient MSI and FortiClient MST are saved
- Create a new task sequence
- Deploy the task sequence

Note that these steps may vary based on your configuration on Microsoft SCCM.

Knowledge Check

1. Which of the following can deploy FortiClient?
 - ✓ A. Microsoft AD server
 - B. FortiClient Configurator Tool

2. What are the steps to deploy a FortiClient from the Microsoft SCCM?
 - ✓ A. Map the network drive where FortiClient MSI is saved, create a new task sequence, and then deploy the task sequence.
 - B. Create a distribution point, configure a group policy, and then assign the package.

Lesson Overview

- ✓ Identify Methods of Provisioning a Standalone FortiClient
- ✓ Understand and configure FortiClient XML
- ✓ Create Custom FortiClient Installation Packages
- ✓ Identify Methods of Deploying FortiClient
- Uninstall FortiClient

FORTINET

Good job! You now understand how to deploy FortiClient.

Now, you will learn how to uninstall FortiClient.

Uninstalling FortiClient

Objectives

- Identify methods of uninstalling FortiClient

FORTINET

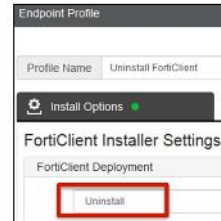
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in uninstalling FortiClient, you will be able to uninstall FortiClient on the management computer.

DO NOT REPRINT
© FORTINET

Uninstall FortiClient

- Standard installation
 - Windows
 - Control panel > Programs and Features
 - Mac OS X
 - Drag the FortiClient application from **Applications directory** to the trash
- FortiClient EMS
 - Creating uninstall endpoint profile
 - Apply to domain or workgroup
 - FortiClient must be password unlock
- Microsoft AD using Group Policy Management
- Microsoft SCCM 2012 using task sequence
 - wmic product where name="FortiClient" call uninstall /nointeractive



The uninstall process is similar to uninstalling any software from your computer. For Windows, you can uninstall FortiClient in **Add/Remove programs** on the **Control Panel**.

For Mac OS X, drag the FortiClient application from **Applications directory** to the trash.

You can also uninstall FortiClient from the EMS by creating an endpoint profile containing a predefined uninstall installer and applying the uninstaller to the workgroup or domain. FortiClient must be password unlock.

You can uninstall FortiClient from Microsoft AD using Group Policy Management or from Microsoft SCCM 2012 using task sequence.

When you select custom features to install, only the modules you select are installed. To enable other features, you will need to uninstall FortiClient, and reinstall an MSI file that includes these features in the installer.

Lesson Overview

- ✓ Identify Methods of Provisioning a Standalone FortiClient
- ✓ Understand and Configure FortiClient XML
- ✓ Create Custom FortiClient Installation Packages
- ✓ Identify Methods of Deploying FortiClient
- ✓ Uninstall FortiClient

FORTINET

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Review

- ✓ Identified methods of provisioning a standalone FortiClient
- ✓ Understand and configure FortiClient XML
- ✓ Create custom FortiClient installation packages
- ✓ Identify methods of deploying FortiClient
- ✓ Methods of uninstalling FortiClient

FORTINET

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to provision and deploy a standalone FortiClient in your existing network to manage the security of multiple endpoints.

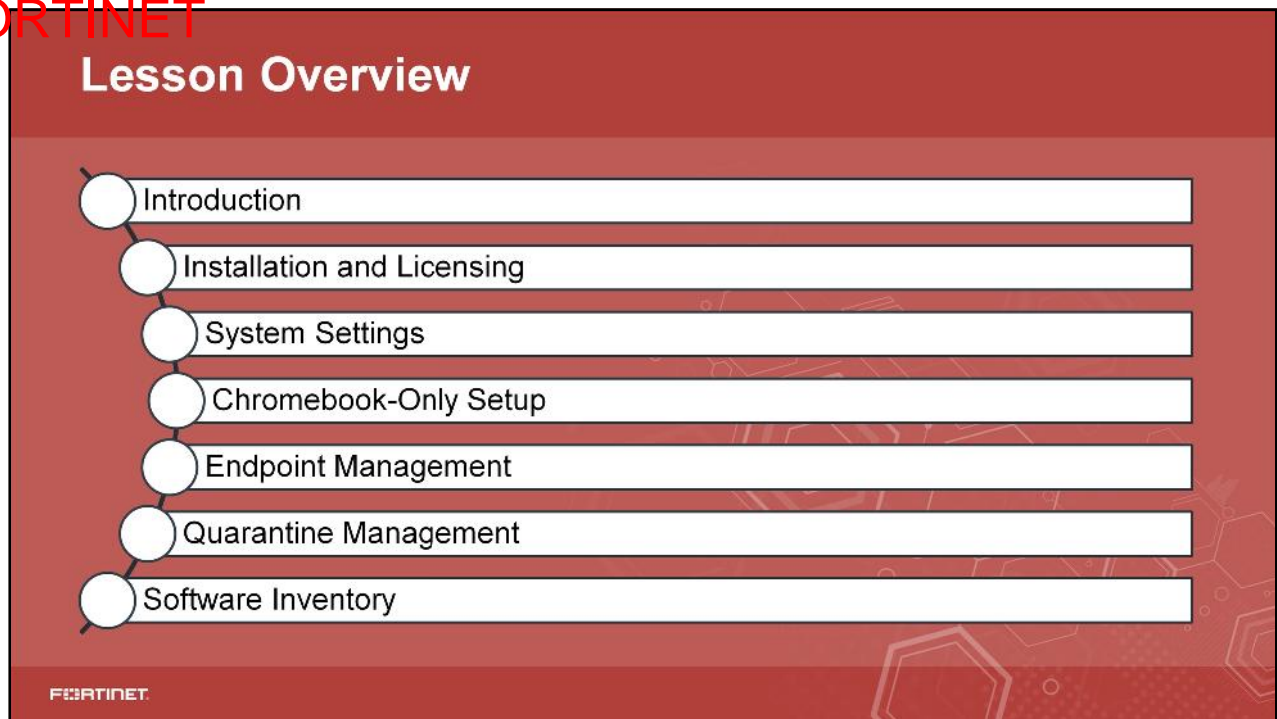
DO NOT REPRINT
© FORTINET



In this lesson, you will learn how to install, configure, and administer FortiClientEMS. You will also learn how to manage a large number of endpoints.

Although this lesson introduces the main FortiClient EMS components and key features, its objectives are about understanding and implementing these features.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn about the topics shown on this slide.

Introduction

Objectives

- Understand the purpose of FortiClient EMS
- Identify FortiClient EMS components
- Understand FortiClient administration and database management

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the purpose, components, and management functions of FortiClient EMS, you will be able to understand the FortiClient EMS purpose, FortiClient EMS administration and database management and identify its components.

DO NOT REPRINT

© FORTINET

FortiClient EMS

- FortiClient EMS is a security management solution that enables:
 - Scalable and centralized management of multiple endpoints (computers).
 - Efficient and effective administration of endpoints running FortiClient
- Provides visibility across the network to securely share information and assign security profiles to endpoints
- Works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users
- Designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints and/or provide web filtering for Google Chromebook users

FORTINET

4

FortiClient EMS is a security management solution that enables scalable and centralized management of multiple endpoints (computers). It also provides efficient and effective administration of endpoints running FortiClient, and visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

FortiClient EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

The benefits of deploying FortiClient EMS include:

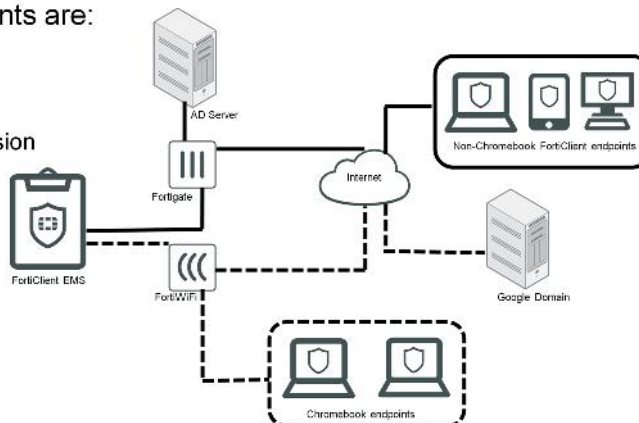
- Remotely deploying FortiClient software to Windows computer
- Updating profiles for endpoint users regardless of access location
- Administering FortiClient endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing and monitoring endpoints, such as status, system, and signature information
- Identifying outdated versions of FortiClient software
- Defining web filtering rules in a profile and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints

You can manage endpoint security for Windows and macOS platforms using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view. FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

DO NOT REPRINT
© FORTINET

FortiClient EMS—Components

- FortiClient EMS provides the infrastructure to install and manage FortiClient software on endpoints
- FortiClient protects endpoints from viruses, threats, and risks
- FortiClient EMS components are:
 - FortiClient EMS
 - Database
 - FortiClient
 - FortiClient Web Filter extension



FORTINET

5

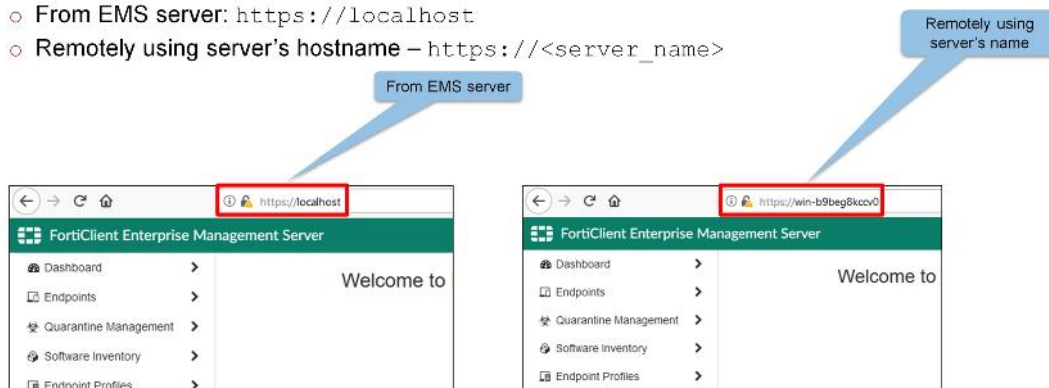
The following components make up FortiClient EMS:

- **FortiClient EMS:** Manages FortiClient on endpoints that connect to your network. It also manages the FortiClient Web Filter extension installed on Google Chromebook endpoints, which are connected to your Google domain. It includes two types of softwares:
 - Console software that manages security profiles, FortiClient on endpoints, and Chromebook endpoints.
 - Server software that provides secure communication between endpoints and the console and between Chromebook endpoints and the Google Admin console.
- **Database:** Stores security profiles and events. Also stores user information retrieved from the Google Admin console for Chromebooks. The SQL database is installed as part of the FortiClient EMS installation.
- **FortiClient:** Helps enforce security and protection on endpoints. It runs on servers, desktops, and portable computers you want to secure.
- **FortiClient Web Filter extension:** Communicates with FortiClient EMS and enforces web filtering on Google Chromebook endpoints.

DO NOT REPRINT
© FORTINET

FortiClient EMS—Access

- FortiClient EMS can be accessed from the GUI by launching the application
- Access using a web browser
 - From EMS server: `https://localhost`
 - Remotely using server's hostname – `https://<server_name>`



There are multiple ways to access FortiClient EMS:

- By launching the FortiClient EMS application
- By using a supported web browser instead of the GUI:
 - From the EMS server by typing `https://localhost` in the web browser
 - Remotely by using the server's hostname `https://<server_name>`

Tip: You can get the `<server_name>` by running `ipconfig /all` on the server. Your **Host Name** will appear under the Windows IP configuration. If you are unable to access the server remotely, make sure you are able to ping `<server_name>`, which can be achieved by adding it to the DNS entry or Windows host file. You may have to modify the firewall rules to allow the connection.

DO NOT REPRINT

© FORTINET

FortiClient EMS—Administration

- Default user account is admin
 - It has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment
 - The admin user has access to all configured Windows and LDAP servers and users and has the authority to configure user privileges and permissions
 - By default, the admin user account has no password; you should add a password to increase security
- You can view the default admin and all users added to FortiClient EMS on
 - **Administration > Administrators**



FORTINET

7

The default user named *admin* has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment. The *admin* user has access to all configured Windows and LDAP servers and users and has the authority to configure user privileges and permissions. If you are not authorized for certain tasks or devices, the related menu items, items in content pages, and buttons are hidden or disabled. In addition, a message informs you that you do not have permission to view the selected information or perform the selected operation.

DO NOT REPRINT

© FORTINET

FortiClient EMS—Administration (Contd)

- You can configure Windows and LDAP user accounts
- Windows users list is derived from the host server on which FortiClient EMS is installed
- LDAP users list is derived from those in the AD domain imported into EMS

FORTINET

8

You can configure Windows and LDAP admin user accounts. Windows users list is derived from the host server on which FortiClient EMS is installed. The LDAP users list is derived from those in the AD domain imported into EMS.

You configure the following settings:

- **User:** Select the Windows/LDAP user to configure permissions for FortiClient EMS.
- **Super Administrator permissions:** Enable the super administrator feature to give the new Windows/LDAP user super administrator permissions.
- **Domain Access:** Select or add access to a domain for the Windows/LDAP user and configure their permissions. If you choose one or more domains in the domain access field, you must select specific permissions.
- **General Permissions:** Use the following settings to configure permissions on FortiClient EMS for the selected Windows/LDAP user
 - Create/Update/Delete LDAPs
 - Create/Update/Delete custom groups
 - Create/Delete filters
- **Endpoint Permissions:** Use the following options to configure permissions for the selected Windows user.
 - Block/Unblock/Quarantine/Unquarantine/Reregister endpoints
 - Run commands on endpoints
 - Access Software Management
 - Access CA Certificate Management
- **Policy Permissions:**
 - Assign/Unassign policies
 - Create/Update/Delete policies

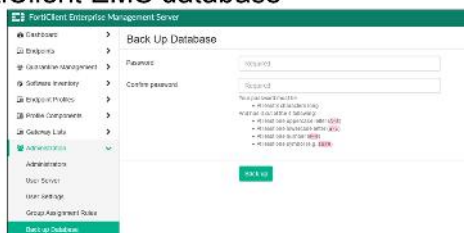
DO NOT REPRINT
© FORTINET

FortiClient EMS—Database Management

- You can back up and restore the FortiClient EMS database

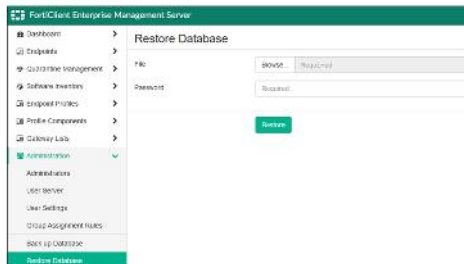
- Backing up the database:

- Administration > Back up Database



- Restoring the database:

- Administration > Restore Database



Backing up the database:

- Click **Administration > Back up Database**.
- Set the following options:-
 - Password:** Enter a password for backing up and restoring the database
 - Confirm password:** Re-enter the password to confirm it
- Click **Back up**.
FortiClient EMS backs up the database

Restoring the database:

- Click **Administration > Restore Database**.
- Click **Browse**.
- Locate the database backup file, and then click **Open**.
- In the **Password**, enter the password used to back up the database.
- Click **Restore**.
When the database is restored, a message appears. The message instructs you to wait for the restored database to reload.
- Wait for the restored database reload.

Note that restore will only work if the database was backed up using the same version number.

- Shows system information, endpoints information, configuration and summary information about vulnerability scans on endpoints



10

You can view the following information on the dashboard:

- FortiClient 6.0 Study Guide

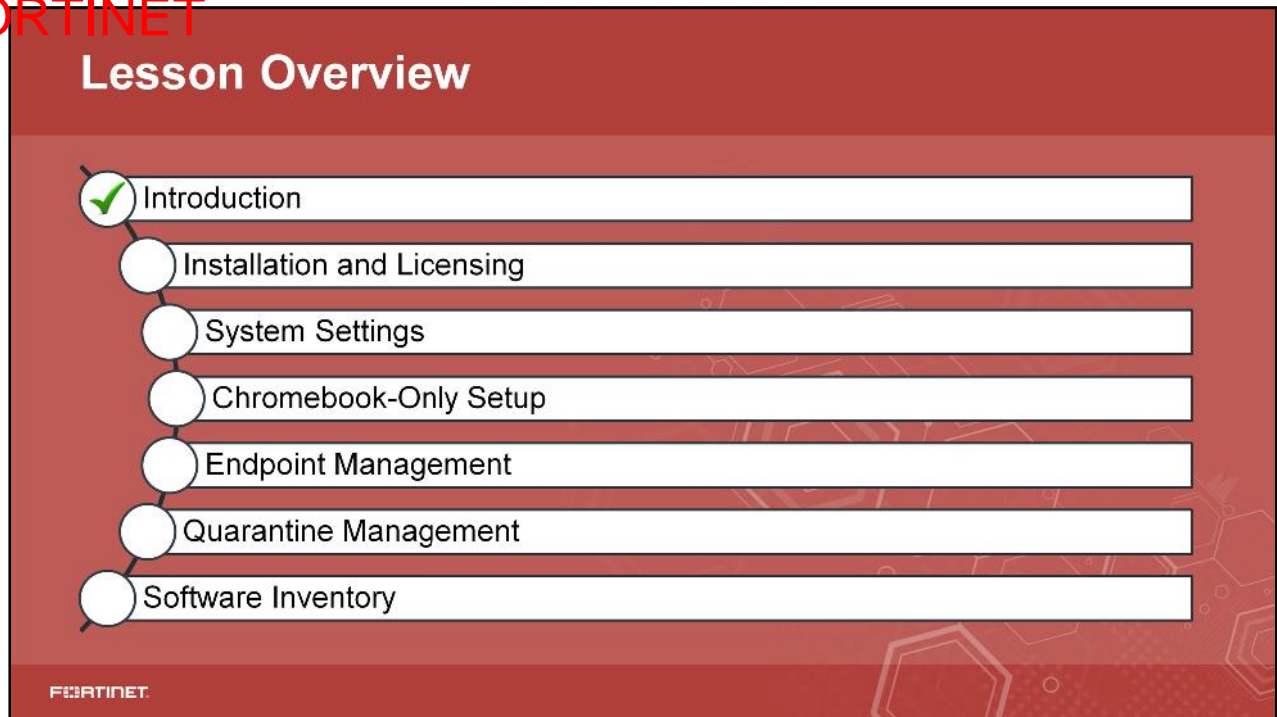
DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which of the following are FortiClient EMS components?
 - A. FortiGate
 - ✓ B. FortiClient
2. What is the default administrator account password?
 - A. Fortinet
 - ✓ B. No-password

DO NOT REPRINT
© FORTINET



Good job! You now know why do we need FortiClient EMS in the enterprise. You also learned about FortiClient EMS components, and understand FortiClient administration and database management.

Now, you will learn about system requirements, license types, service ports, and installation options for FortiClient EMS.

DO NOT REPRINT
© FORTINET

Installation and Licensing

Objectives

- Understand system requirements
- Identify license types
- Identify services and ports
- Identify the FortiClient EMS installation file
- Understand installation using a GUI and CLI

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in installing and licensing FortiClient EMS, you will be able to understand system requirements, identify license types, services and ports. You will also learn about FortiClient EMS installation file and how to install using GUI and CLI.

DO NOT REPRINT
© FORTINET

FortiClient EMS—System

- **System requirements:**

- The minimum system requirements for FortiClient EMS are as follows:

- Microsoft Windows Server 2008 R2 or later
- 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)
- 4 GB RAM (8 GB RAM or more is recommended)
- 40 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Internet access

- **Management capacity:**

- FortiClient EMS is intended for use by enterprises. It has the capacity to manage a large number of endpoints. Fortinet recommends you have at least 200 GB of disk space available.

FORTINET

14

You should read the *FortiClient EMS Release Notes* to become familiar with the relevant software components and other important information about the product.

Internet Access: Internet access is required during installation. This becomes optional once installation is complete. FortiClient EMS accesses the Internet to obtain information about FortiGuard engine and signature updates.

Note that you should only install FortiClient EMS and the default services for the operating system on the server. You should not install additional services on the same server as FortiClient EMS.

DO NOT REPRINT

© FORTINET

FortiClient EMS—Licenses

- **Free trial license:**
 - When you install FortiClient EMS, the free trial license is enabled by default. There are separate licenses for all the platforms except Chromebook.
- **Purchased license:**
 - There are separate purchasable licenses for Chromebook management and all the other platforms.
- **Add-on FortiGate endpoint license:**
 - To enforce endpoint compliance on the firewall.

FORTINET

15

Free trial license: The free trial license for Windows, MacOS, and Linux FortiClient EMS supports ten FortiClient endpoints. FortiClient EMS consumes one license count for each managed FortiClient device. The free trial license for Chromebook management supports ten Google Chromebook users. FortiClient EMS consumes one license count for each logged-in user. If the user logs out, the license seat times out (the default timeout is 24 hours), and the license is released. At this point, another user can use this license seat.

Purchased license: Each purchased Windows, MacOS, Linux, and Google Chromebook users license allows the management of one FortiClient endpoint. You must purchase a minimum of 100 endpoint licenses, and you can have these EMS licenses for a maximum three-year term.

- **Add-on FortiGate endpoint license:** You can use a licensed FortiClient EMS to deploy, provision, and manage FortiClient endpoints. However, if you have a FortiGate in your network, you can buy an add-on FortiGate endpoint license to enforce endpoint compliance on the firewall while EMS is managing the endpoints. Using FortiGate with EMS is optional.
- **Extending license expiries:** You can apply multiple licenses to FortiClient EMS to extend the license expiry. For example, say you purchase two one-year licenses for FortiClient EMS. After you register and apply the first license, FortiClient EMS has an expiry date of September 5, 2018. You can register and apply the second license as a renewal, after which FortiClient EMS has an expiry date of September 5, 2019. You must upload the second license file to FortiClient EMS using the GUI. Registering the license does not automatically update the license expiry on FortiClient EMS. Note that using a second license to extend the license expiry date does not increase the number of clients. To increase the number of licensed clients, contact Fortinet Support for a `co-term` contract .

FortiClient EMS—Services and Ports

- You must enable the required ports and services for use by FortiClient EMS and its associated applications on your server

FortiClient EMS services and ports to manage endpoints

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient Telemetry	FortiClient endpoint management	TCP	8013 (default)	Incoming	Installer/GUI
Sanitization (SMB) service	FortiClient EMS uses the SMB service during FortiClient initial deployment.	TCP	445	Outgoing	N/A
Distributed Computing Environment / Remote Procedure Calls (DCE-RPC)	The EMS server connects to endpoints using RPC for FortiClient initial deployment.	TCP	135	Outgoing	N/A
Active Directory server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636 (LDAPS)	Outgoing	GUI
FortiClient download	Downloading FortiClient installer created by the EMS server	TCP	10443 (default)	Incoming	Installer
Apache/HTTPS	Web access to EMS	TCP	443	Incoming	Installer
FortiGuard	FortiGuard antivirus, vulnerability, and application version updates	TCP	80	Outgoing	N/A
SMTP server/email	Alerts for EMS and endpoint events. When an alert is triggered, an email notification is sent.	TCP	25 (default)	Outgoing	GUI
FortiClient endpoint probing	FortiClient EMS uses ICMP for endpoint probing during FortiClient initial deployment.	ICMP	N/A	Outgoing	N/A

FortiClient EMS services and ports to manage Chromebooks

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient on Chrome OS	Connection to EMS	TCP	8443 (default) You can customize this port.	Incoming	GUI
G suite API/Google domain directory	API calls to retrieve Google domain information	TCP	443	Outgoing	N/A

The following ports and services should be enabled for use on Chromebooks when using FortiClient for Chromebooks:

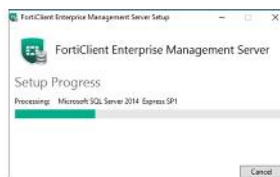
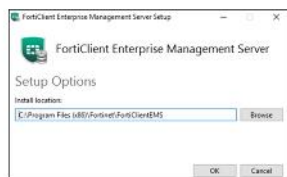
Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient EMS	Connection to profile server	TCP	8443 (default)	Outgoing	Via Google Admin console when adding the profile
FortiGuard	URL rating	TCP	443, 3400	Outgoing	N/A
FortiAnalyzer	Send logs to FortiAnalyzer	TCP	8443	Outgoing	N/A

The required ports and services enable FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable port 8013 and port 10443 because the FortiClient EMS installation opens these.

DO NOT REPRINT
© FORTINET

FortiClient EMS—Installation File

- Installation file is available for download from the Fortinet Support website
 - FortiClientEnterpriseManagement_6.0.X.<build>_x64.exe
- You can also receive the installation file from a sales representative
- FortiClient EMS installation package includes:
 - FortiClient EMS
 - Microsoft SQL Server 2014 Express Edition
 - Apache HTTP server



FORTINET

17

FortiClient EMS is available for download from the Fortinet Support website. You can also receive the installation file from a sales representative. The following installation file is available for FortiClient EMS: **FortiClientEnterpriseManagement_6.0.X.<build>_x64.exe**.

Note that local administrator rights and Internet access are required to install FortiClient EMS.

DO NOT REPRINT

© FORTINET

FortiClient EMS—Installation Using the CLI

- You can install FortiClient EMS using the CLI
- CLI Options are:
 - AllowedWebHostnames
 - ApacheServerAdminEmail
 - BackupDir
 - ClientDownloadPort
 - RemoteManagementPort
 - InstallFolder
 - InstallSQL
 - ScriptDB
 - ServerHostname
 - SQLAuthType
 - SQLCmdlineOptions="/INSTANCEDIR"

FORTINET

18

You can install FortiClient EMS using the CLI.

AllowedWebHostnames: The default value is localhost, 127.0.0.1. To clear this value, first enter `AllowedWebHostnames=*`, then enter the desired `AllowedWebHostnames` value. Otherwise, the value entered will be appended to [localhost, 127.0.0.1], so that `AllowedWebHostNames=localhost,127.0.01,<new_value>`.

ApacheServerAdminEmail: Enter the Apache Server administrator's email address. By default, this is `admin@yourcompany.com`.

BackupDir: Enter the desired backup directory path for SQL server.

ClientDownloadPort: Enter the HTTP port number. The default is 80.

RemoteManagementPort: Enter the HTTPS port number. The default is 443.

InstallFolder: Specify the directory to install EMS to.

InstallSQL: Controls whether the installer will install SQL Server Express on the same server as FortiClient EMS. Enter 1 to install SQL Server Express; otherwise, enter 0. By default, SQL Server Express is installed with FortiClient EMS.

ScriptDB: Controls where the installer will attempt to create the database from db scripts. Enter 1 to create the database from db scripts. You should enter 0 only if databases have already been set up on the server and you are only installing EMS components locally.

ServerHostname: Enter the preferred hostname (the remote hostname). The default is the local host.

SQLAuthType: Enter `sql`.

SQLCmdlineOptions="/INSTANCEDIR": Enter the desired directory to install SQL Server Express to.

For details on other CLI commands, please refer to the *FortiClient EMS Administration Guide*.

DO NOT REPRINT

© FORTINET

Installation Using the CLI (Contd)

- CLI Options:
 - SQLCmdlineOptions="/INSTANCENAME"
 - SQLEncryptConnection
 - SQLPort
 - SQLServer
 - SQLServerInstance
 - SQLService
 - SQLTrustServerCertificate
 - SQLUser
 - SQLUserPassword
 - WindowsUser
 - WindowsUserPassword
- Allows you to enable specific options during installation, such as customizing the SQL Server Express installation directory, using custom port numbers, and so on

FORTINET

19

Installation using the CLI allows you to enable specific options during installation, such as customizing the SQL Server Express installation directory, using custom port numbers, and so on.

Example: Allowing remote access to FortiClient EMS and using custom port numbers.

- To allow remote access to FortiClient EMS from a web browser, install FortiClient EMS by entering the following command in the CLI. You can also specify custom HTTP and HTTPS port numbers:


```
FortiClientEnterpriseManagement_6.0.3.XXXX_x64.exe
ServerHostname =<preferred_host_name>
ClientDownloadPort = <HTTP_port_number>
RemoteManagementPort = <HTTPS_port_number>
AllowedWebHostnames = <allowed_web_host_names>
ApacheServerAdminEmail = <Apache_Server_admin_email_address>
```
- The example below specifies the server host name as `emshost.ems.com`, appends `emshost.ems.com` to the allowed web host names, and specifies `example@example.com` as the Apache server administrator email. In this example, the HTTP and HTTPS ports are changed to 1080 and 22443, respectively.


```
FortiClientEnterpriseManagement_6.0.3.XXXX_x64.exe
ServerHostname = emshost.ems.com
ClientDownloadPort = 1080
RemoteManagementPort = 22443
AllowedWebHostnames = emshost.ems.com
ApacheServerAdminEmail = example@example.com
```

DO NOT REPRINT

© FORTINET

FortiClient EMS—Uninstalling

- To uninstall use **Programs and Features**
 - Click **Start > Control Panel > Programs > Uninstall a program**
 - Select **FortiClient Enterprise Management Server**, and click **Uninstall**
 - Follow the uninstallation wizard prompts
- FortiClient EMS has dependencies on other applications

FORTINET

20

Use the **Programs and Features** pane of the Microsoft Windows Control Panel to uninstall FortiClient EMS. FortiClient EMS installs the following dependencies. If other applications on the same computer are not using them, you can uninstall them manually after removing FortiClient EMS:

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0
- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL S

DO NOT REPRINT

© FORTINET

Knowledge Check

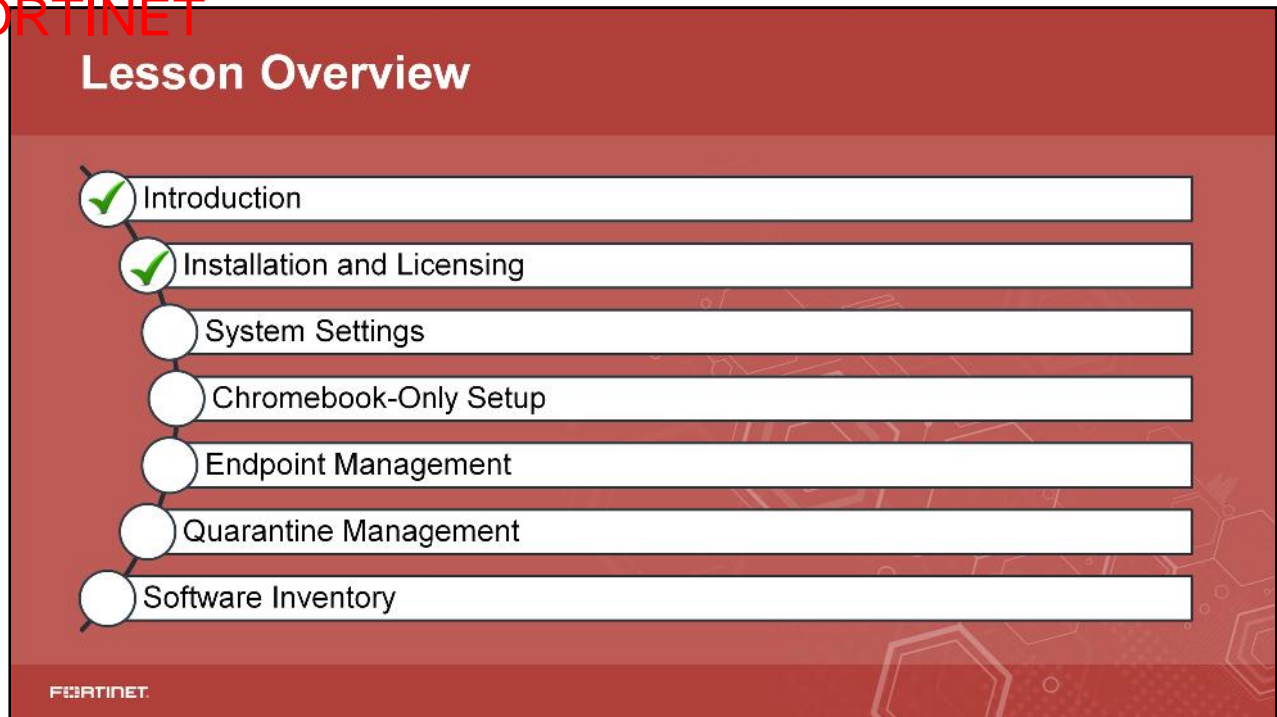
1. What minimum disk space does Fortinet require for FortiClient EMS?

- ✓ A. 40GB
- B. 200GB

2. Which port is used by FortiClient for Telemetry?

- A. 10443
- ✓ B. 8013

DO NOT REPRINT
© FORTINET



Good job! You now understand the system requirements to install FortiClient EMS. You also learned about license types, services, the FortiClient EMS installation file, as well as how to install FortiClient EMS using the GUI and CLI.

Now, you will learn about the FortiClient EMS system settings.

System Settings

Objectives

- Discuss FortiClient EMS settings
- Configure server settings
- Configure logs settings
- Configure banner and alerts

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient EMS system settings, you will be able to configure the following:

- Server
- Logs
- FortiGuard
- Endpoints
- Login banner
- EMS alerts
- Endpoint alerts
- SMTP server
- Custom messages

System Settings—Server

- You can change the default IP address and port and configure other server settings for FortiClient EMS

- System Settings > Server**

- Shared Settings:**
 - Shared between EMS managing Windows, MacOS, Linux endpoints, and Chromebook endpoints

System Settings > Server > Shared Settings

Shared Settings

- Hostname:** Displays the FortiClient EMS server's host name.
- Listen on IP:** Displays the IP addresses for the FortiClient EMS server. FortiClient connects to FortiClient EMS on the specified IP address
- Use FQDN:** Turn on to specify a fully qualified domain name (FQDN) for the FortiClient EMS server.
 - FQDN:** Displayed when **Use FQDN** is turned on. Enter the FQDN for the FortiClient EMS server. FortiClient can connect using the specified IP address in the **Listen on IP Addresses** field or the specified FQDN.
- Remote HTTPS access:** Specify settings for remote administration access to FortiClient EMS. Turn remote HTTPS access to FortiClient EMS console on and off. The following options are available when you select the **Remote HTTPS access** check box:
 - Pre-defined hostname:** Displays the pre-defined host name. You cannot change the name.
 - Custom hostname:** Displays the pre-defined host name of the server on which FortiClient EMS is installed. You can customize the host name. When you change the host name, the web server restarts.
 - Redirect HTTP request to HTTPS:** If you select this check box and you attempt to remotely access EMS at `http://<server_name>`, this URL is automatically redirected to `https://<server_name>`.
- SSL certificate:** Displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, the page displays the **Replace** button.

DO NOT REPRINT

© FORTINET

System Settings—Server

• EMS Settings:

- These settings are used by FortiClient EMS managing Windows, MacOS, and Linux endpoints

• EMS for Chromebooks Settings

- These settings are used by FortiClient EMS managing Chromebook endpoints

System Settings > Server > EMS Settings

The screenshot shows the 'System Settings > Server > EMS Settings' page. It contains two main sections: 'EMS Settings' and 'EMS for Chromebooks Settings'. The 'EMS Settings' section includes fields for 'Listen on port' (8083), 'DHCP onnet/offnet' (radio buttons), 'Enable TLS 1.0/1.1' (radio buttons), 'FortiClient download URL' (text field with a dropdown), and 'Sign software packages' (checkbox). The 'EMS for Chromebooks Settings' section includes fields for 'Listen on port' (8443), 'User inactivity timeout' (24 hours), 'Profile update interval' (300 seconds), 'SSL certificate' (No certificate imported), and 'Service account' (account-id@forticlientwebfilter.lan).

FORTINET

25

EMS Settings

- **Listen on port:** Displays the default port for the FortiClient EMS server. You can change the port by typing a new port number. FortiClient connects using the specified port.
- **DHCP onnet/offnet:** Enable to monitor endpoints within the company network (on-net). Endpoints that are connected to FortiClient EMS from outside the company network are off-net endpoints.
- **Enable TLS 1.0/1.1:** Enable TLS 1.0 and 1.1 for file downloads. Windows 7 uses old TLS versions.
- **FortiClient download URL:** FortiClient installers created on FortiClient EMS will be made available for download at the URL.
- **Sign software packages:** Select this checkbox to have Windows FortiClient software installers created by or uploaded to EMS digitally signed with a code signing certificate.

EMS for Chromebooks Settings

- **Listen on port:** Displays the default port for the FortiClient EMS server for Chromebooks. You can change the port by typing a new port number. The FortiClient Web Filter extension on Chromebooks connects to FortiClient EMS using the specified port number.
- **User inactivity timeout:** Enter the number of hours of inactivity after which to time out the user.
- **Profile update interval:** Specify the profile update interval (in seconds).
- **SSL certificate:** Displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, the page displays **Replace** button.
- **Certificate:** Browse and upload a new SSL certificate file.
- **Password:** Configure a new SSL password.
- **Service account:** Displays the service account ID currently in use. You must enter an account ID and Private key to update account. Note that you must add an SSL certificate to FortiClient EMS to allow Chromebooks to connect to EMS.

System Settings—Logs

- You can specify what level of log messages to capture
- You can specify when to automatically delete logs and alerts

System Setting > Logs

Logs

Log level Info

Clear logs every 30 days Clear now

Clear alerts every 30 days Clear now

Clear events every 30 days Clear now

Clear Chromebook events every 7 days Clear now

This applies to Chromebooks only.

Save

FORTINET

29

In **System Settings>Logs** you can specify what level of log messages to capture in the logs for FortiClient EMS. You can also specify when to automatically delete logs and alerts.

- Log level:** Select the level of messages to include in FortiClient EMS logs. For example, if you select **Info**, all log messages from **Info** to **Emergency** are added to the FortiClient EMS logs.
- Clear logs every:** Enter the number of days that you want to store logs. For example, if you enter 30, logs will be stored for 30 days. Any logs older than 30 days are automatically deleted.
- Clear alerts every:** Enter the number of days that you want to keep alerts. For example, if you enter 30, alerts will be kept for 30 days. Any alerts older than 30 days are automatically deleted.
- Clear events every:** Enter the number of days that you want to keep events. For example, if you enter 30, events will be kept for 30 days. Any events older than 30 days are automatically deleted.
- Clear Chromebook events every:** Enter the number of days that you want to keep Chromebook events. For example, if you enter 30, Chromebook events will be kept for 30 days. Any Chromebook events older than 30 days are automatically deleted.
- Clear now:** Click to immediately delete all FortiClient EMS logs or alerts.

System Settings—FortiGuard and Endpoints

• System Settings > FortiGuard

• System Settings > Endpoints

FORTINET

27

FortiGuard

- **Server Location:** Configure FortiGuard server location to **Nearest** or **US**.
 - If you select **Nearest**, FortiClient EMS connects to the FortiGuard server whose IP address is provided by the DNS server.
 - If you select **US**, FortiClient EMS can connect only to FortiGuard servers available in the United States and does not attempt to access a FortiGuard server outside the U.S.
- **FortiManager:** Use FortiManager for client software/signature updates. The **Failover** enables failover to FDN when FortiManager for FortiClient is not available.

Endpoints

- **FortiClient telemetry connection key:** Add the FortiClient telemetry connection key for FortiClient EMS. FortiClient must provide this key during connection.
- **Keep alive interval:** Each connected FortiClient endpoint sends a short keep-alive message to FortiClient EMS at the specified interval.
- **Full keep alive interval:** Each connected FortiClient endpoint sends a full keep-alive message to FortiClient EMS at the specified interval.
- **License timeout:** Each connected FortiClient endpoint consumes a license seat
 - If an endpoint disconnects from EMS, the license seat is retained in anticipation that the endpoint will reconnect. If the endpoint does not reconnect within the given time out, its connection record is removed from EMS.
 - If the endpoint is removed, switched off, or goes offline, and does not re-establish a telemetry connection to EMS within the given time out, the endpoint is deleted from EMS even if FortiClient on the endpoint shows that it is still connected.
- **Automatically upload avatars:** If you select this check box, FortiClient uploads user avatars to all of the devices
- **Allow duplicate FCT registrations:** If you select this check box, this setting allows duplicate FortiClient registrations by assigning the duplicate registrations new UUIDs.

System Settings—Banner and Alerts

• Login Banner

- System Settings > Login Banner
- A message appears before a user logs in to EMS

• EMS Alerts

- System Settings > EMS Alerts
- Send alerts for EMS events

When you select the **Enable login banner** check box, a message appears on the login screen before a user logs in to EMS.

1. Click **System Settings > Login Banner**.
2. Click **Enable login banner**.
3. In the **Message** field, type your message.
The **Preview** section displays a preview of the message.
4. Click **Save**.

EMS Alerts:

- **Version Alerts**
 - New EMS version is available for deployment
 - New FortiClient version is available for deployment
- **FortiClient Alerts**
 - EMS license is expired or about to expire
 - EMS fails to sync with LDAP domains
 - Less than 10% of client licenses are left
 - Client licenses have run out
 - New software is detected
- **FortiClient for Chromebook Alerts**
 - EMS license for Chromebooks is expired or about to expire
 - Less than 10% of the client licenses for Chromebooks are left
 - Client licenses for Chromebooks have run out

DO NOT REPRINT

© FORTINET

System Settings—Banner and Alerts

• Endpoints Alerts

- System Settings > Endpoint Alerts
- Send alerts for EMS events

FORTINET

29

Endpoints Alerts:

- System Settings > Endpoint Alerts
- Select the following events to send email for:
 - Malware is detected
 - Repeated malware is detected (same malware is detected on the same machine within the last 24 hours)
 - Multiple malwares are detected (different malwares are detected on the same machine within the last 24 hours)
 - Malware outbreak is detected (same malware is detected on different endpoints within the last 24 hours)
 - Zero-day malware is detected by FortiSandbox
 - C&C attack communication channel is detected
 - Critical vulnerability is detected
 - Endpoint FortiClient Telemetry is manually disconnected by user
 - Endpoint signature database is out-of-date
 - Endpoint software is out-of-date
 - Endpoint is not compliant

System Settings—SMTP Server

- **SMTP Server**

- **System Settings > SMTP Server**
- When an alert is triggered, EMS sends an email notification to the configured email address(es)

The screenshot shows the 'SMTP Server' configuration window. It contains the following fields and options:

- Server:** A text input field with a 'Required' label.
- Port:** A text input field with the value '25'.
- Security:** A row of buttons: 'None' (highlighted in green), 'STARTTLS', 'SMTPS', and 'Auto Detect' (with a checkmark icon).
- From:** A text input field with the label 'Optional'.
- Reply-to:** A text input field with the label 'Optional'.
- Subject:** A text input field with the value 'Alert Email from EMS Server'.
- Recipients:** A text input field with the placeholder 'Press enter to add a new value...'.
- Test subject:** A text input field with the value 'Test Email from EMS Server'.
- Save:** A green button at the bottom right.

SMTP Server:

- **System Settings > SMTP Server**
- You can set up an SMTP server to enable alerts for EMS and endpoint events
 - **Server:** Enter the SMTP server.
 - **Port:** Enter the port number.
 - **Security:** Select **None**, **STARTTLS**, or **SMTPS** for the security type, or select the **Auto Detect** button to automatically select the security type. If you select **STARTTLS** or **SMTPS**, the **Username** and **Password** boxes become available.
 - **From:** Enter the email address to send the alerts from.
 - **Reply-To:** Enter the email address to send the replies to.
 - **Subject:** The subject of the sent email alert.
 - **Recipients:** Enter email address(es) to send alerts to. Press **Enter** to add more email addresses.
 - **Test subject:** Test email's subject.
 - **Test message:** Test email's message.
 - **Test recipient:** Email address to send the test email to.
 - **Send Test Email:** Click the button to test the configured email settings.

DO NOT REPRINT

© FORTINET

System Settings—Alerts

- Viewing alerts
You can view alerts FortiClient EMS generates by clicking a bell icon. Examples of events that generate an alert include:
 - New version of FortiClient is available
 - FortiClient deployment failed
 - Failure to check for signature updates
 - Error encountered when downloading AD server entries
 - Error encountered when scanning for local computers
- Customize endpoint quarantine message
 - You can customize the message that displays on an endpoint when it has been quarantined by FortiClient EMS
 - This feature is supported only for endpoints running FortiClient version 6.0.0 and later

FORTINET

31

Viewing Alerts:

- You can view the alerts FortiClient EMS generates. Examples of events that generate an alert include:
 - New version of FortiClient is available
 - FortiClient deployment failed
 - Failure to check for signature updates
- A red label is associated with the **Alert** icon when new notifications are available or received. It is cleared when you view the alert.
 - Click the **Alert** icon (a bell) in the toolbar.
 - Click the **Filter** icon in each column heading to apply filters.
 - Click **Clear Filters** to remove the filters
- Customize endpoint quarantine message
 1. Click **System Settings > Custom Messages**.
 2. Select **Endpoint Quarantine Message**.
 3. In the **Message** field, enter the desired message. You can enter up to 512 characters. The **Preview** section displays the custom message as it would appear on the latest version of FortiClient. You can also use the **Preview** slider to zoom in and out on the message preview.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. By default, which port does FortiClient EMS managing a Chromebook endpoint listen on?
☒ A. 8443
☐ B. 8013

2. Which of the following are FortiGuard server locations?
☐ A. US or EMEA
☒ B. US or Nearest

DO NOT REPRINT
© FORTINET



Good job! You now understand the system settings for FortiClient EMS.

Now, you will learn how to set up FortiClient EMS for Chromebook only.

Chromebook-Only Setup

Objectives

- Discuss Google admin console setup
- Configure service account credentials

FORTINET

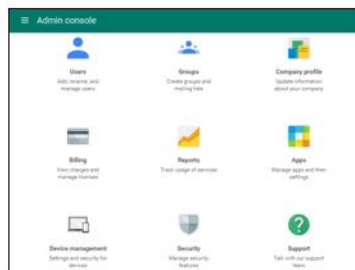
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in setting up FortiClient EMS to manage Chromebooks, you will be able to configure the Google admin console setup and service account credentials.

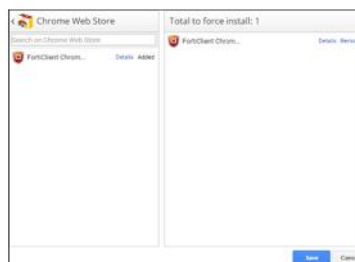
DO NOT REPRINT
© FORTINET

Chromebook-only Setup—Admin Console Setup

- Logging in to the Google Admin console



- Add FortiClient Web Filter extension



FORTINET

35

Log in to the Google admin console using your Google domain admin or G Suite account. Note that a Google account set up through an organization like work, school, a club, or maybe family or friends, is called G Suite account.

Adding the FortiClient Web Filter extension:

1. On the Google Admin console, click **Device management > Chrome Management > User Settings > Apps and Extensions > Force-installed Apps and Extensions > Manage force-installed apps**.
2. Select **Chrome Web Store**, and search for the following extension ID:
`igbgpehnbmhdgjbhkkpedommgmfbeao`
3. Add the extension ID, and then click **Save**.
The extension name displays as **FortiClient Chromebook Web Filter Extension**.

DO NOT REPRINT

© FORTINET

Chromebook-Only Setup—Admin Console Setup

- Configure the FortiClient Web Filter extension to enable communication
- FortiClient EMS hosts the services that assign endpoint profiles of web filtering policies
- FortiClient EMS is the profile server

FORTINET

39

You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS. FortiClient EMS hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS also handles the logs and web access statistics sent from the FortiClient Web Filter extensions.

Configuration:

1. On FortiClient EMS, click **System Settings** > **Server** to locate the server name and port.
2. Create a text file that contains the following text:


```
{
  "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >" }
}
```

 For example:


```
{
  "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443" }
}
```
3. On the Google Admin console, click **Device management** > **Chrome Management** > **App Management** > **FortiClient Chrome Web Filter Extension** > **User settings**.
4. Click a domain or organization unit (OU).
5. In the right pane, under **Configure**, upload a new configuration file. You can also view the current settings.
6. Click **Save**.
7. Click **Device Management** > **Chrome** > **App Management** to view your configured Chrome apps.

DO NOT REPRINT

© FORTINET

Chromebook-Only Setup—Add Root Certificates

- Add root certificates
 - Chromebook needs to trust EMS certificate
- FortiClient extensions use HTTPS connections to communicate
- HTTPS connections require SSL certificates

FORTINET

37

Add certificates:

- The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS using HTTPS connections.
- You must obtain an SSL certificate and add it to FortiClient EMS to allow the Chromebook extension to trust FortiClient EMS.
- If you use a public SSL certificate, you need to add only the public SSL certificate to FortiClient EMS.
- If you prefer to use a certificate that is not from a common certificate authority CA, you must add the SSL certificate to FortiClient EMS and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS will not work.

For more details about certificates, see the *FortiClientEMS Administration Guide*.

DO NOT REPRINT
© FORTINET

Chromebook-Only Setup—Admin Console Setup

- Disable access to Chrome developer tools:
 1. On the Admin console, go to **Device management > Chrome Management > User Settings**.
 2. For the **Developer Tools** option, select **Never allow use of built-in developer tools**.
- Disallow incognito mode:
 1. On the Admin console, click **Device management > Chrome management > User settings**.
 2. On the panel on the left side of the page, select the organization.
 3. In the **Security** section, set **Incognito Mode** to **Disallow incognito mode**.
 4. Click **Save**.
- Disallow guest mode:
 1. On the Admin console, click **Device management > Chrome management > Device settings > Sign-in settings**.
 2. On the panel on the left side of the page, select the organization.
 3. Under **Guest Mode**, in the **Allow Guest Mode** drop-down list, select **Do not allow guest mode**.
 4. Click **Save**.

FORTINET

38

You should disable access to Chrome developer tools. This blocks users from disabling the FortiClient Web Filter extension.

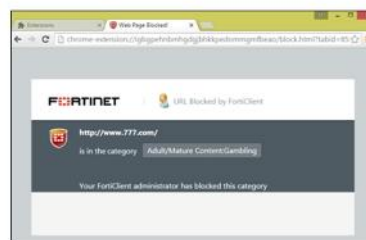
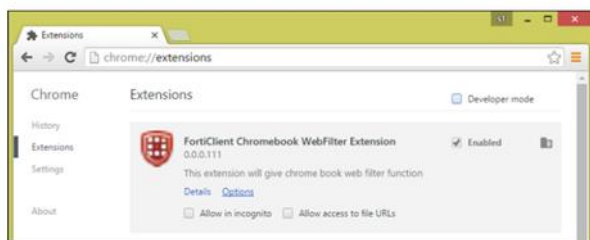
When users browse in incognito mode, extensions are bypassed. You should disallow incognito mode for managed Google domains.

You should disallow guest mode for managed Google domains.

DO NOT REPRINT
© FORTINET

Chromebook-Only Setup—Admin Console Setup

- Block Task Manager:
 1. On the Google Admin console, click **Device Management > Chrome Management > User settings > Apps and Extensions**.
 2. On the panel on the left side of the page, select the organization.
 3. Under **Task Manager**, in the drop-down list, select **Block users from ending processes with the Chrome Task Manager**.
 4. Verify FortiClient Web Filter



FORTINET

39

You should block **Task Manager** for managed Google domains. After you add the Google domain to FortiClient EMS, the Google Admin console automatically pushes the FortiClient Web Filter extension to the Chromebooks when users log in to the Google domain.

You can verify that the feature has become available on the Chromebooks.

1. Open the Google Chrome browser.
2. Enter the following address in the address bar: `chrome://extensions`.
3. Visit any gambling site, such as `http://www.777.com`, and confirm the site is blocked.

DO NOT REPRINT
© FORTINET

Chromebook-Only Setup—Service Account

- FortiClient EMS includes the following default service account credentials generated by the Google Developer console:

Option	Default setting	Where used
Client ID	102515977741391213738	Google Admin console
Email address	account-1@forticlientwebfilter.iam.gserviceaccount.com	FortiClient EMS
Service account certificate	A certificate in .pem format for the service account credentials	FortiClient EMS

- Must add the client ID's default value to the Google Admin console—no other configuration for service account credentials is required
- Add service account credentials to the Google Admin console and EMS
- Fortinet recommends unique service account credentials for improved security

FORTINET

40

FortiClient EMS requires service account credentials generated by the Google Developer console. You can use the default service account credentials provided with FortiClient EMS. To configure the default service account credentials, you must add the client ID's default value to the Google Admin console. No other configuration for service account credentials is required. These settings allow Google to trust FortiClient EMS, which enables FortiClient EMS to retrieve information from the Google domain.

- On the Google Admin console, click **Security** > **Advanced settings** (you may need to click "Show more" to see this) > **Manage API client access**.
- Set the following options:
 - For the **Client Name** option, add the client ID from the service account credentials.
 - For the **API Scopes** option, add the following string:
`https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly`
- Click **Authorize**.

Note that the service account credentials are a set. If you change one credential, you must change the other two credentials.

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS:

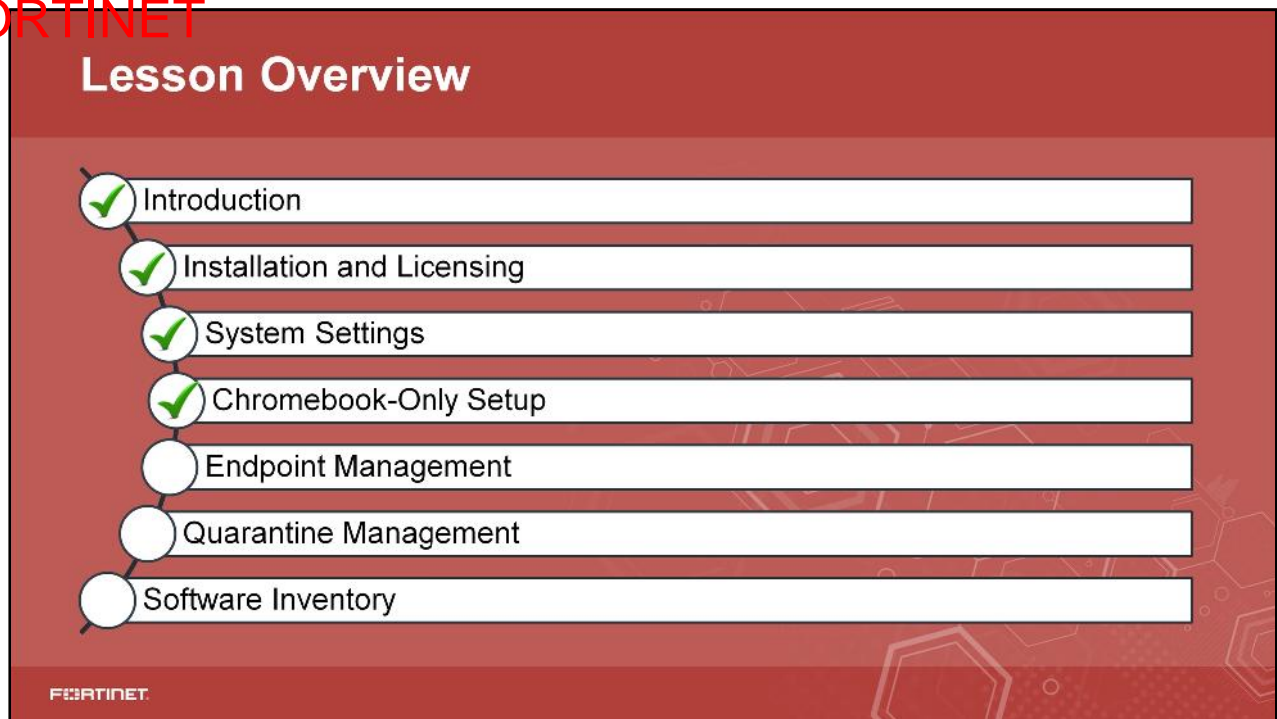
- Create unique service account credentials using the Google Developer console.
- Add the unique service account credentials to the Google Admin console.
- Add the unique service account credentials to FortiClient EMS.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What type of Google account do you need to access the Google Admin console?
✓ A. G Suite
B. Personal
2. What connection does FortiClient Chromebook web filter extension use to communicate?
✓ A. HTTPS
B. HTTP

DO NOT REPRINT
© FORTINET



Good job! You now understand how to configure FortiClient EMS to manage Chromebooks.

Now, you will learn about endpoint management.

Endpoint Management

Objectives

- Configure Windows MacOS and Linux endpoints
- Configure Google domains

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiClient for endpoint management, you will be able to configure Windows, Mac OS and Linux endpoints, as well as Google domains.

DO NOT REPRINT

© FORTINET

FortiClient EMS—Endpoint Management

- Windows MacOS and Linux endpoints
 - FortiClient EMS needs to determine which devices to manage
 - Information can come from an Active Directory (AD) server, Windows workgroup, or manual FortiClient connection
- Creating groups
 - You can create groups to organize endpoints
 - You can also rename and delete groups
- Adding endpoints
 - You can add endpoints using an AD service
 - Endpoint users can manually connect FortiClient Telemetry to FortiClient EMS

FORTINET

44

FortiClient EMS needs to identify which devices to manage. For Windows, and macOS, device information can come from an AD server, Windows workgroup, or manual FortiClient connection. Linux endpoint doesn't communicate with AD server.

Click **Endpoints**, right-click a domain or workgroup to create, and then rename and delete groups.

Adding endpoints:

- Adding endpoints using an AD domain server:
 - You can import endpoints manually from an AD server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying endpoints that are part of an AD domain server.
 - On EMS, click **Endpoints > Manage Domains > Add**.

Note that after importing endpoints from an AD server, you can edit the endpoints. These changes are not synced back to the AD server.

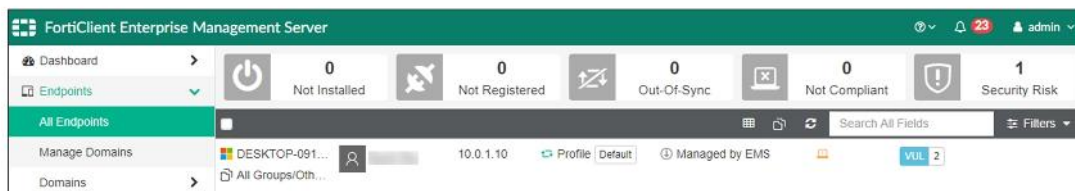
- Connecting manually from FortiClient:
 - Endpoint users can manually connect FortiClient Telemetry to FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient.
 - This process is sometimes called registering FortiClient to FortiClient EMS.

DO NOT REPRINT
© FORTINET

FortiClient EMS—Endpoint Management

- Viewing endpoints

- You can view the list of endpoints in a domain or workgroup on the **Endpoints** pane
- You can view details about each endpoint on the **Client Details** pane



After you add endpoints to FortiClient EMS, you can view the list of endpoints in a domain or workgroup on the **Endpoints** pane.

You can also view details about each endpoint on the **Client Details** pane, and use filters to access endpoints with specific qualities.

You can save filter settings as bookmarks, then select the bookmarks to use them.

DO NOT REPRINT

© FORTINET

FortiClient EMS—Endpoint Management

- You can manage the following on the **Endpoints** pane:

- Running antivirus scans on endpoints
- Running vulnerability scans on endpoints
- Patching vulnerabilities on endpoints
- Uploading FortiClient logs
- Running the FortiClient diagnostic tool
- Updating signatures
- Disconnecting and connecting endpoints
- Quarantining endpoints
- Excluding endpoints from management
- Deleting endpoints



FORTINET

49

On the Endpoints pane, you can do the following:

- A full or quick AntiVirus scan on endpoints. Scanning starts on the endpoints with the next FortiClient Telemetry communication.
- A vulnerability scan on endpoints. You can view the history of vulnerability scans for each endpoint on the **Client Details** pane.
- FortiClient patch detected critical and high vulnerabilities on endpoints.
- FortiClient can automatically patch many software:
 - If a vulnerability requires the endpoint user to download and install a software to patch a vulnerability, the FortiClient Console displays the information.
- FortiClient upload a log file from one or several endpoints to FortiClient EMS:
 - The log file is uploaded to the hard drive on the computer running EMS.
 - The uploaded log file is not visible in the FortiClient EMS GUI.
- EMS runs the FortiClient Diagnostic Tool on one or multiple endpoints and export the results to the hard drive on the computer on which you are running FortiClient EMS:
 - The exported information is not visible in the FortiClient EMS GUI.
- EMS request the FortiClient update signatures on the endpoints.
- Manually disconnect and connect endpoints using EMS:
 - From the **Action** menu, select **Deregister** to disconnect.
 - From the **Action** menu, select **Register** to connect.
- EMS can quarantine endpoints. Quarantined endpoints cannot access the network.
- EMS can exclude endpoints from management:
 - Right-click a domain or workgroup and select **Exclude from management**
- Disconnect endpoints from EMS:
 - Disconnect **Registered** endpoint first.
 - From the **Action** menu, select **Delete Device**.

DO NOT REPRINT

© FORTINET

FortiClient EMS—Endpoint Management

- You can quarantine an endpoint from FortiOS using EMS using an API
- The following network components are required:
 - FortiGate
 - FortiAnalyzer
 - FortiClient EMS
 - FortiClient
- Security Fabric, which includes the above network devices, can automatically quarantine an endpoint on which an indicator of compromise (IoC) is detected

FORTINET

47

The Security Fabric offers visibility of endpoints at various monitoring levels. This configuration functions as follows:

1. FortiClient sends logs to FortiAnalyzer.
2. FortiAnalyzer discovers IoCs in the logs and notifies the FortiGate.
3. FortiGate identifies if the FortiClient is a connected endpoint and if it has the login credentials for the EMS that FortiClient is connected to.
 - A. With this information, FortiGate sends a notification to EMS to quarantine the endpoint
4. EMS searches for the endpoint and sends a quarantine message to it
5. The endpoint receives the quarantine message and quarantines itself, blocking all network traffic.
 - A. The endpoint notifies the FortiGate and EMS of the status change

Executing automation:

The following command triggers the quarantine action on the endpoint at `<endpoint_ip_address>`

- `diag endpoint forticlient-ems-rest-api queue-quarantine-ipv4 <endpoint_ip_address>`

Note that feature is not supported on FortiClient (Linux).

DO NOT REPRINT

© FORTINET

FortiClient EMS—Endpoint Management (Contd)

- FortiClient must connect to both the EMS and FortiGate
- FortiGate must have EMS IP address and credentials to login
- FortiAnalyzer must receive logs from both FortiGate and FortiClient

FORTINET

48

The following lists the prerequisites that must be met for FortiClient, EMS, and FortiGate

FortiClient:

- FortiClient must be installed on the endpoint and connected to both EMS and FortiGate

EMS:

- A profile must be assigned to the endpoint.
- A gateway list using the FortiGate's IP address must be assigned to the endpoint.
- The **Remote HTTPS access** must be enabled.

FortiGate

Before automation can be triggered, you must configure the following:

- Automation objects:
 - Automation trigger
 - You can create an automation trigger by entering the CLI command `config system automation-trigger .`
 - Automation action
 - You can create an automation action by entering the CLI command `config system automation-action.`
 - Automation stitch
 - You can create automation stitch by entering the CLI command `config system automation-stitch.`
 - EMS firewall address object
 - You can create an EMS firewall address object by entering the CLI command `config firewall address.`
 - Endpoint control FCT-EMS object
 - You can create an endpoint control FCT-EMS object by entering the CLI command `config endpoint-control forticlient-ems.`

DO NOT REPRINT

© FORTINET

FortiClient EMS—Endpoint Management

- Provisioning FortiClient Android endpoints for central management
 - Use a third-party QR code generator to create a QR code to distribute to FortiClient (Android) users
 - Scan the QR code from their devices
 - QR codes can contain the FortiClient EMS server's hostname or IP address, port number, and a connection key
- Google Domains
 - **Google Domains** is only available if FortiClient EMS manage Chromebooks
 - You can add, view, edit, and delete domains

FORTINET

49

You can use a third-party QR code generator to create a QR code to distribute to FortiClient (Android) users. FortiClient (Android) users can scan the QR code from their devices to automatically enable FortiTelemetry and attempt a connection to the specified FortiClient EMS server and FortiGate. QR codes can contain the FortiClient EMS server's hostname or IP address, port number, and a connection key. Only the FortiClient EMS hostname/IP address is required; all other fields are optional.

FortiClient EMS needs to identify which devices to manage. Device information comes from the Google Admin console. **Google Domains** is only available if **EMS for Chromebooks Settings** is selected in **System Settings > Server**.

You can add domains by clicking **Google Domains > Manage Domains**, and clicking **Add**. After you add domains to FortiClient EMS, you can view, edit, and delete.

Note that section is only applicable if you are using FortiClient EMS to manage Google Chromebooks.

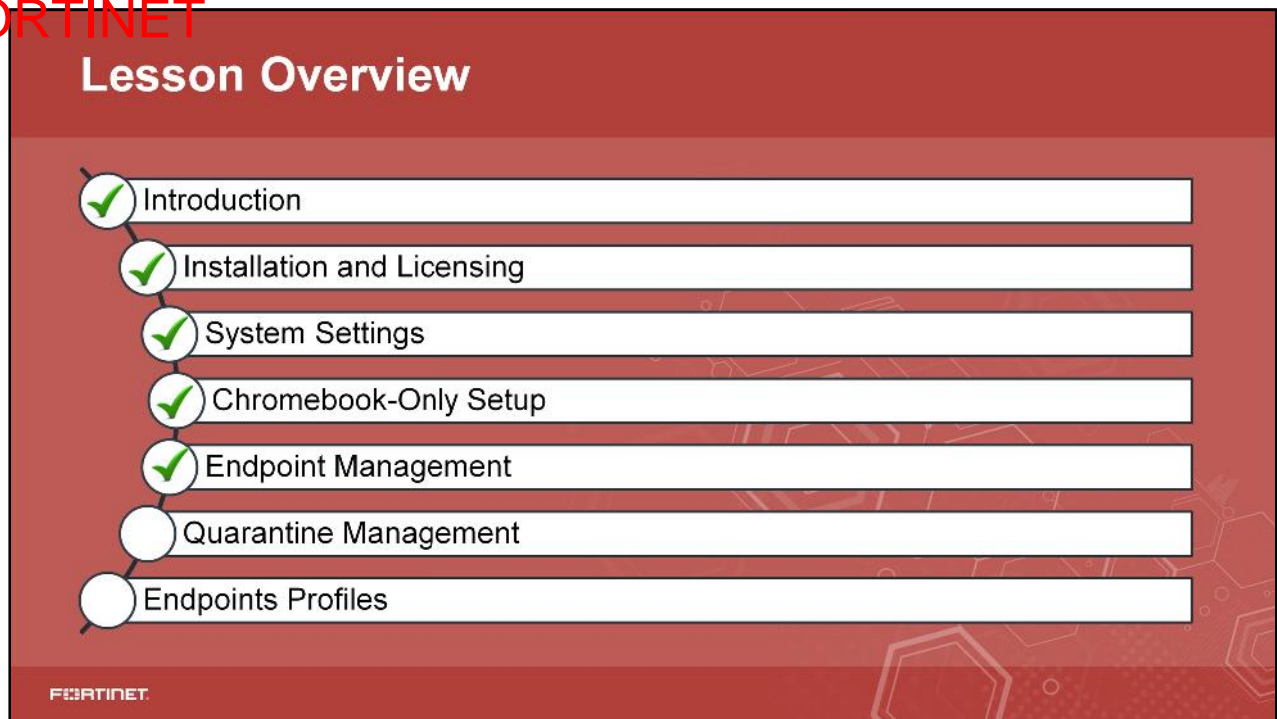
DO NOT REPRINT
© FORTINET

Knowledge Check

1. What are the two methods to add endpoints to FortiClient EMS?
 - ✓ A. Microsoft Active Directory (AD) server and manual connection from FortiClient
 - B. Import XML configuration from FortiGate and FortiClient

2. Which of the following network components are required to enable FortiOS to quarantine an endpoint?
 - A. Chromebook Web Filter extension
 - ✓ B. FortiGate, FortiAnalyzer, FortiClient EMS, and FortiClient

DO NOT REPRINT
© FORTINET



Good job! You now understand endpoint management for Windows, macOS, Linux, and Chromebook user endpoints on FortiClient EMS.

Now, you will learn about quarantine management.

Quarantine Management

Objectives

- View quarantined files
- Whitelist quarantined files

FORTINET


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiClient EMS to manage quarantined files, you will be able to view and whitelist quarantined files.

DO NOT REPRINT
© FORTINET

Quarantine Management—View and Whitelist Files

- Viewing quarantined files
 - FortiClient sends quarantined file information to FortiClient EMS
 - You can view the list of quarantined files in the **Files** pane
 - You can filter the file list
- Whitelist quarantined file
 - You can whitelist and restore quarantined files
 - You can view the lost whitelisted files in the **Whitelist** pane
 - You can filter, edit the file description, and delete whitelisted files


59

The FortiClient EMS administrator can view quarantined file information for all managed endpoints on the **Files** pane and whitelist files from FortiClient EMS if needed.

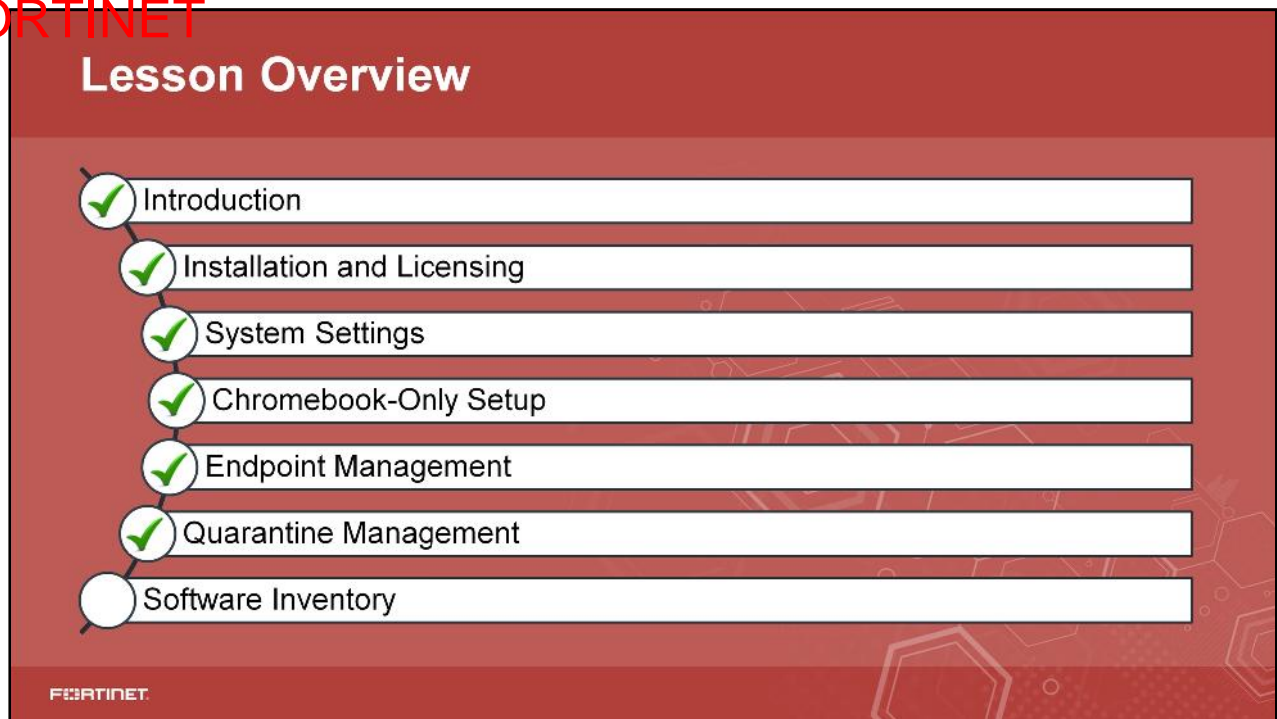
FortiClient sends quarantined file information to FortiClient EMS. After FortiClient quarantines files on endpoints and sends the quarantined file information to FortiClient EMS, you can view the list of quarantined files in the **Files** pane. You can also view details about each quarantined file and use filters to access quarantined files that have specific qualities.

- **Quarantine Management > Files:** The list of quarantined files, a quick status bar, and a toolbar display in the content pane.

You can whitelist and restore quarantined files. This releases the files from quarantine and makes them accessible on the endpoint with the next Telemetry communication between FortiClient EMS and FortiClient.

1. Click **Quarantine Management > Files**.
2. Select the files you want.
3. Click **Whitelist & Restore**.
4. In the confirmation dialog, click **Yes**, and then **Okay**.
The file status changes to **Quarantined & Whitelisted**.

DO NOT REPRINT
© FORTINET



Good job! You now understand how FortiClient EMS manages quarantined files.

Now, you will learn how FortiClient EMS manages the software inventory on endpoints.

DO NOT REPRINT
© FORTINET

Software Inventory

Objectives

- View installed applications

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using FortiClient EMS to view the software inventory on endpoints, you will be able to determine what applications are installed.

DO NOT REPRINT
© FORTINET

Software Inventory—Applications

- You can centrally view a list of software installed on all endpoints
- The list includes details for each application, such as vendor and version information
- Applications**
 - Shows information about installed applications for all managed endpoints
 - You can filter by application

Name	Vendor	Version	First Detected	Last Installed	Install Count
FortiClient	Fortinet Inc.	6.0.0.0036	2018-04-15	2018-04-10	1
Google Chrome	Google Inc.	65.0.3325.181	2018-04-15	2018-04-15	1
Mozilla Firefox 59.0.2 (x64 en-US)	Mozilla	59.0.2	2018-04-15		1
Mozilla Maintenance Service	Mozilla	59.0.2	2018-04-15		1
Notepad++ (64-bit x64)	Notepad++ Team	7.5.6	2018-04-15		1
Skype version 8.19	Skype Technologies S.A.	8.19	2018-04-15	2018-04-15	1

FortiClient

59

You can centrally view a list of software installed on all endpoints. The list includes details for each application, such as vendor and version information. You can view this information by application or vendor on the **Applications** pane, or by host on the **Hosts** pane. FortiClient sends installed application information to FortiClient EMS.

The FortiClient EMS administrator can view installed application information for all managed endpoints on the **Applications** pane.

- Software Inventory > Applications**

Total Applications: Number of applications that have been installed on all managed endpoints. Click to display the list of installed applications.

Total Vendors: Number of vendors whose applications have been installed on managed endpoints. Click to display the list of installed applications sorted by vendor.

New Detections: Number of applications that have been detected as newly installed since the last Telemetry communication. Click to display newly detected applications sorted by date detected.

Display by: Select to toggle between the following options:

- Display applications alphabetically by application name.
- Sort applications by vendor name.

Refresh: Click to refresh the list of applications on the **Content** pane.

Clear Filters: Click to clear all filters applied to the list of files.

Name: This is the name of the installed application.

Vendor: This is the name of the installed application's vendor.

Version: This is the version number of the installed application.

First Detected: This is the date the application was first detected as installed on the endpoint.

Last Installed: This is the date the application was last installed on an endpoint.

Install Count: This is the number of endpoints the application is installed on.

You can apply filters by application name, vendor name, and version number.

DO NOT REPRINT
© FORTINET

Software Inventory—Hosts

- **Hosts**

- Shows information about installed application for all managed endpoints by host
- You can filter by host

Host	User	OS	IP	Application Count	Last Installation
WIN-1F38OCJBW4	Administrator	Microsoft Windows Server 2012 R2 Standard	10.0.4.102	6	2018-04-10

Name	Vendor	Version	Install Date
FortiClient	Fortinet Inc.	6.0.0.0035	2018-04-10
Google Chrome	Google Inc.	65.0.3325.181	2018-04-10
Mozilla Firefox 59.0.2 (64-bit)	Mozilla	59.0.2	2018-04-10
Microsoft Maintenance Service	Mozilla	59.0.2	2018-04-10
Notepad++ (64-bit x64)	Notepad++ Team	7.5.5	2018-04-10
Skype version 8.19	Skype Technologies S.A.	8.19	2018-04-10

FORTINET

57

The FortiClient EMS administrator can view installed applications information for all managed endpoints by host on the **Hosts** pane.

- **Software Inventory > Hosts**

Applications: Number of applications that have been installed on all managed endpoints

Operating Systems: Number of different operating systems on managed endpoints

View Details: Displays list of software installed on the selected endpoint

Refresh: Click to refresh the list of applications in the content pane

Clear Filters: Click to clear all filters applied to the list of files

Host: Host name

User: Name of the endpoint user

OS: Operating system installed on the endpoint

IP: IP address of the endpoint

Application Count: Number of applications installed on the endpoint

Last Installation: Date of the most recent application installation on the endpoint

You can apply filters by host name, user name, OS name, and IP address.

DO NOT REPRINT
© FORTINET



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

Review

- ✓ Understand the purpose of FortiClient EMS, FortiClient administration and database management, and identify EMS components
- ✓ Understand system requirements, license types and installation using a GUI and CLI
- ✓ Understand FortiClient EMS settings
- ✓ FortiClient EMS Chromebook-Only Setup
- ✓ FortiClient EMS Endpoint management
- ✓ FortiClient EMS Quarantine management
- ✓ FortiClient Software inventory

FORTINET

This slide shows the objectives that you covered in this lesson.

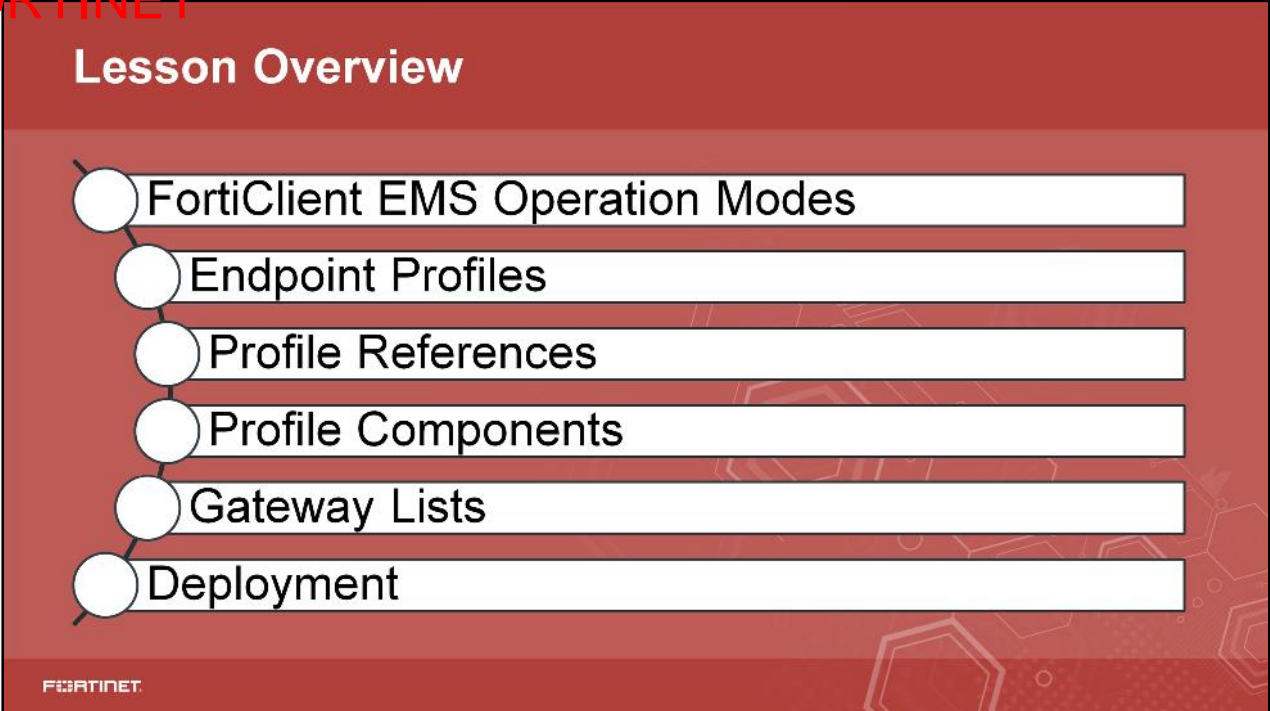
By mastering the objectives covered in this lesson, you learned how to install, configure, and administer FortiClient EMS. You also learned how to manage a large number of endpoints.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn how to deploy, provision, and manage FortiClient on endpoints using FortiClient EMS.

DO NOT REPRINT
© FORTINET



Lesson Overview

- FortiClient EMS Operation Modes
- Endpoint Profiles
- Profile References
- Profile Components
- Gateway Lists
- Deployment

FORTINET

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT
© FORTINET

FortiClient EMS: Operation Modes

Objectives

- Understand FortiClient EMS operation modes

FORTINET

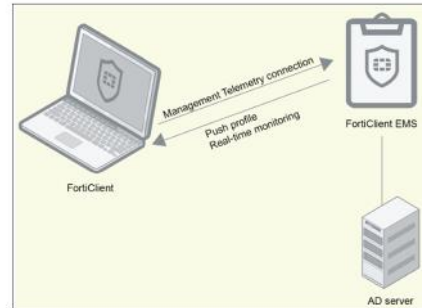
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence understanding FortiClient EMS, you will be able to use it effectively in your network.

DO NOT REPRINT
© FORTINET

Standalone Mode Without Security Fabric

- FortiClient EMS provides FortiClient endpoint provisioning
- FortiClient endpoints connect FortiClient Telemetry to FortiClient EMS to receive configuration information from FortiClient EMS
- Does not support compliance
- Endpoint status shows as **Managed by EMS**



FORTINET

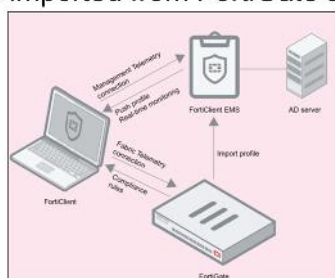
4

FortiClient EMS in standalone mode provides FortiClient endpoint provisioning. FortiClient endpoints connect FortiClient telemetry to FortiClient EMS to receive configuration information from FortiClient EMS. This operation mode does not support compliance.

DO NOT REPRINT
© FORTINET

Integrated Mode With Security Fabric

- FortiClient EMS provides FortiClient endpoint provisioning
- FortiGate provides compliance rules to the endpoint
- FortiClient endpoints connect FortiClient Telemetry:
 - To receive configuration information from FortiClient EMS
 - To receive compliance rules from FortiGate
- Profiles can also be imported from FortiGate and FortiManager to FortiClient EMS



FORTINET

5

You can integrate FortiGate with FortiClient EMS. When used together, FortiGate performs endpoint control and network access compliance (NAC), and FortiClient EMS deploys and manages FortiClient software on endpoints.

When FortiGate is configured for NAC, you can use FortiOS to create a FortiClient compliance profile that defines compliance rules and non-compliance action. The compliance rules define what configuration FortiClient software and the endpoint must have for the endpoint to maintain access to the network through FortiGate.

FortiOS 6.0.0 and later versions use one of the following two methods to determine endpoint compliance. The FortiOS configuration determines which one of the following two methods is used:

- An endpoint is considered compliant if FortiClient is managed by the EMS server authorized on FortiOS
- An endpoint is considered compliant if it complies with the specific compliance rules configured on FortiOS

FortiOS versions earlier than 6.0.0 determine an endpoint to be compliant if it complies with the compliance rules configured in FortiOS. The non-compliance action defines what action FortiGate takes when endpoints fail to comply with the compliance rules. When the non-compliance action is **block**, FortiGate blocks endpoints from accessing the network when they fail to comply with the compliance rules. When the non-compliance action is **warn**, FortiGate warns the endpoint about non-compliance, but allows network access after the endpoint user acknowledges the warning.

DO NOT REPRINT
© FORTINET

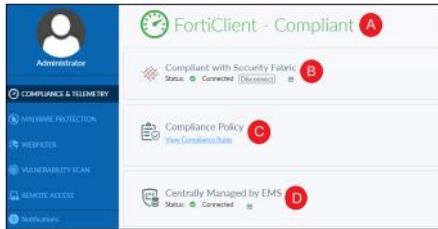
Integrated Mode With Security Fabric

- When viewing the endpoint in the FortiClient EMS GUI, the endpoint's connection is shown as

- FortiTelemetry to FGT<number>
- Managed by EMS



- FortiClient GUI



Label A: This shows the endpoint is connected to the specified FortiGate and is compliant to security policy rules defined under FortiClient Compliance profiles on that FortiGate.

Label B: This shows the endpoint is connected to and receiving compliance rules from the specified FortiGate. Click the menu icon to view the FortiGate's IP address, hostname, and serial number.

Label C: When FortiClient Telemetry is connected to FortiGate, you can view the compliance rules from FortiGate. The compliance rules communicate the configuration required for the FortiClient Console and the endpoint to remain compliant. When the endpoint has a non-compliant status, an exclamation mark indicates which compliance rules are not met.

Label D: View the FortiClient EMS server's name. This indicates FortiClient EMS is managing and provisioning configuration to the endpoint. Click the menu icon to view the FortiClient EMS server's IP address, hostname, and serial number.

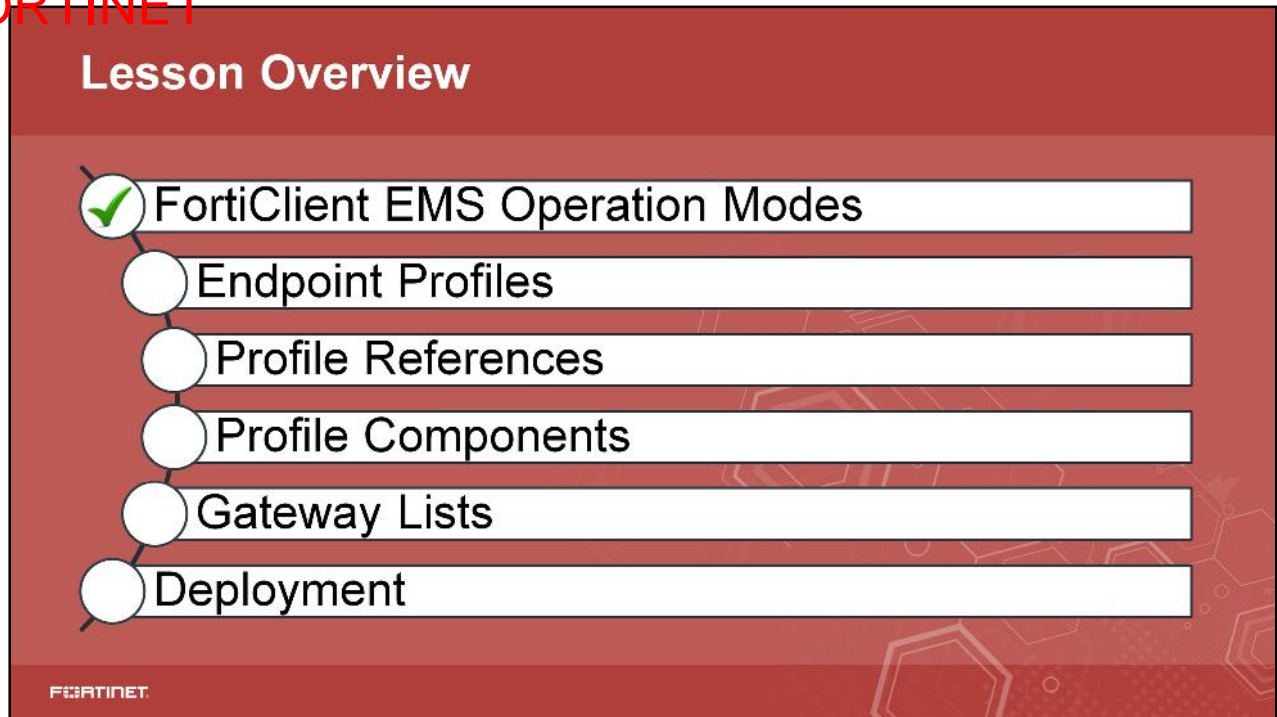
Although the compliance rules define what configuration FortiClient software and the endpoint must have, the FortiClient compliance profile from FortiGate does not include any configuration information. The endpoint user or administrator is responsible for configuring the FortiClient Console to adhere to the compliance rules. An administrator can use FortiClient EMS to configure the FortiClient Console.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which type of information does FortiClient EMS in standalone mode not support?
 - A. FortiClient configuration information
 - ✓ B. FortiClient compliance information
2. Which of these devices provide compliance?
 - ✓ A. FortiGate
 - B. FortiClient EMS

DO NOT REPRINT
© FORTINET



Good job! You now understand FortiClient EMS operation modes.

Now, you will learn about endpoint profiles.

FortiClient EMS: Endpoint Profiles

Objectives

- Configure and edit endpoint profiles
- Assign endpoint profiles
- Manage endpoint profiles

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring, editing, assigning, and managing endpoint profiles, you will be able to use endpoint profiles to define the features installed on FortiClient endpoints.

DO NOT REPRINT
© FORTINET

Edit Default Profile

- When you install FortiClient EMS, a default profile is created
- The default profile is designed to provide effective levels of protection
- There is only one default profile for:
 - Windows
 - macOS
 - Linux endpoints
- Chromebook has a separate default profile because of different supported features
- You can also edit the default profiles

FORTINET

10

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups you create. The default profile is designed to provide effective levels of protection. There are separate default profiles for Windows, macOS, and Linux endpoints and for Chromebook endpoints.

You can create and configure separate profiles for Windows, macOS, and Linux endpoints and for Chromebook endpoints. You can also edit the default profiles.

You can edit to add or remove settings in the default profile. You can revert to the default settings by clicking **Revert to Default**.

- Do one of the following:
 - To edit the default profile for Chromebooks, click **Endpoint Profiles > Local Chromebook Profiles**, and click the **Default - Chromebooks** profile
 - To edit the default profile for other endpoints, click **Endpoint Profiles > Local Profiles**, and click the **Default** profile.
- Configure the settings on the tabs
- Click **Save** to save the profile

DO NOT REPRINT
© FORTINET

Configure and Create Profiles

- To use specific features, such as application firewall, either create a new profile or edit the default profile
- Consider the following when creating profiles:
 - Use default settings within a profile
 - Consider the endpoint's role when changing the default profile or creating new profiles
 - Create a separate group and profile for endpoints requiring long-term special configuration
 - Use FortiClient EMS for all central profile settings, and set options for within the group
 - EMS can only apply profile to a group
- In EMS you can create endpoint profiles to achieve desired settings

FORTINET

11

The default profile is designed to provide effective levels of protection. To use specific features, such as application firewall, create a new profile or edit the default profile.

You can create endpoint profiles to achieve desired settings, such as:

- Profiles to configure FortiClient
- Profiles to deploy FortiClient
- Profiles to uninstall FortiClient

Note that an individual FortiClient must belong to a group before the settings can be pushed to them.

Configure and Create Profiles (Contd)

- Profiles to configure FortiClient
 - A profile that excludes any installation or uninstallation of FortiClient software on endpoints
 - Type use to only configure FortiClient software on endpoints
- Profiles to deploy FortiClient
 - Must create a new profile to deploy FortiClient
 - You cannot add a FortiClient installer to the default profile
- Profiles to uninstall FortiClient
 - You can configure a profile to uninstall FortiClient from endpoints

Endpoint Profiles > Manage Profiles > +Add

FORTINET

12

Profiles to configure FortiClient: This type of profile excludes any installation or uninstallation of FortiClient software on endpoints. This type of profile is used to configure FortiClient software on endpoints. On the **Deployment** tab, leave **FortiClient Deployment** disabled.

Profiles to deploy FortiClient: You must create a new profile to deploy FortiClient to endpoints as you cannot add a FortiClient installer to the default profile. You must also add FortiClient installers to FortiClient EMS before you can select the installers in a profile. The selected FortiClient installer in a profile controls which tabs are displayed for configuration in the profile. Only the tabs for the features in the selected installer are displayed for configuration in the profile. For example, if the installer includes only the VPN feature, only the **VPN** tab is displayed for you to configure. The **System Settings** tab is always displayed. To add a tab, go to **Profile Components > Manage Installers**.

You can disable a feature included in the installer, then enable it later in the profile.

Profiles to uninstall FortiClient: You can configure a profile to uninstall FortiClient from endpoints. You must create a new profile for this configuration. You cannot use the default profile to uninstall FortiClient from endpoints.

DO NOT REPRINT
© FORTINET

Endpoint Profiles—Import Profiles

- Importing FortiGate profiles
 - Endpoint profiles in FortiOS are called FortiClient compliance profiles
 - You can import a FortiClient compliance profile into EMS
- Importing FortiClient profiles from FortiManager
 - You can import FortiClient profiles from FortiManager into EMS

Endpoint Profiles > Manage Profiles > Import

FORTINET

13

Importing FortiGate profiles: In FortiOS, endpoint profiles are called FortiClient compliance profiles. You can import a FortiClient compliance profile into EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or add configuration information that supports FortiGate compliance rules.

To import profiles successfully from FortiOS to FortiClient EMS, the HTTPS port on FortiGate must be open. In FortiOS, click **Network > Interfaces > Administrative Access** and select the **HTTPS** check box.

Importing FortiClient profiles from FortiManager: You can import FortiClient profiles from FortiManager into EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or add configuration information that supports the FortiGate compliance rules.

To import profiles successfully from FortiManager to FortiClient EMS, the HTTPS port on FortiManager must be open. In FortiManager, click **System Settings > Network** and select the **HTTPS** check box.

You need following information to connect:


- **IP address/Hostname:** Enter the IP address and port of the FortiGate or FortiManager device from which the profile is being imported, in the format: **<ip address>:<port>**
- **VDOM:** Enter a VDOM name from the FortiGate/FortiManager if applicable
- **Username:** Enter the FortiGate's or FortiManager's login username
- **Password:** Enter the FortiGate's or FortiManager's login password

DO NOT REPRINT
© FORTINET

Endpoint Profiles

- **Creating profiles with XML**
 - You can configure FortiClient profile settings by using XML or a custom XML configuration file
 - The custom XML file must include all settings required by the endpoint

- **Creating profiles to automatically upgrade FortiClient**
 - You can create a profile to automatically upgrade FortiClient to the latest patch release
 - Profile must be configured with an installer


14

Creating profiles with XML: You can configure FortiClient profile settings in FortiClient EMS by using XML or a custom XML configuration file. The custom XML file must include all settings required by the endpoint at the time of deployment.

1. Click **Endpoint Profiles > Manage Profiles**, and click the **Add** button.
2. In the **Profile Name** field, enter a name for the profile.
3. Click **Advanced**. The **XML Configuration** tab opens, and the profile configuration displays in XML.
4. Click the **XML Configuration** tab, and click **Edit**.
5. Edit the XML.
6. Click **Test XML**.
7. Click **Save** to save the profile.

Creating profiles to automatically upgrade FortiClient: You can create a profile to automatically upgrade FortiClient to the latest patch release. The profile must be configured with an installer that meets the following requirements:

- The FortiClient installer was created in FortiClient EMS 1.2.0 or later
- The FortiClient installer was created with the latest FortiClient version available for selection in FortiClient EMS at the time the installer was created
- The FortiClient installer was created with the **Keep software updated to the latest patch release** option enabled

DO NOT REPRINT
© FORTINET

Profile for Chromebooks

- Chromebook profiles support
 - Web filtering by categories
 - Black and white lists
 - Safe search
- You can create different profiles and assign them to different groups in the Google domain
- Default profile applies to any domains you add
- Viewing profiles
 - Newly created endpoint profiles are listed under **Endpoint Profiles** in the left pane
 - You can view endpoint profiles and their settings

FORTINET

15

Chromebook profiles support web filtering by categories, black and white lists, and safe search. You can create different profiles and assign them to different groups in the Google domain. When you install FortiClient EMS, a default profile is created. This profile is applied to any domains you add to FortiClient EMS.

Enabling/disabling safe search: The search engine provides a safe search feature that blocks inappropriate or explicit images from search results. The safe search feature helps block most adult content. FortiClient EMS supports safe search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS controls the Safe Search feature.

DO NOT REPRINT
© FORTINET

Assigning and Managing Profiles

- You can assign the profile to domains or workgroups
- The profile settings are automatically pushed to the endpoints
- Unassigned domain or workgroup gets default profile
- You can manage profiles from the **Endpoint Profiles** pane
- You can
 - Edit profiles
 - Clone profiles
 - Sync profile changes
 - Edit sync schedules
 - Delete profiles

FORTINET

18

Assigning profiles: After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup. If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied.

Editing profiles: When you edit a profile assigned to endpoints or domains, the changes are automatically pushed to the endpoints or Chromebooks when you save the profile.

Cloning profiles: When you clone a profile, all the content displays in the content pane, and you can give new name to save it.

Syncing profile changes: For profiles imported from FortiGate or FortiManager, you can manually sync profiles so they are updated with the latest changes from the FortiGate or FortiManager they were imported from.

Editing sync schedules: For profiles imported from FortiGate or FortiManager, you can edit the sync schedule.

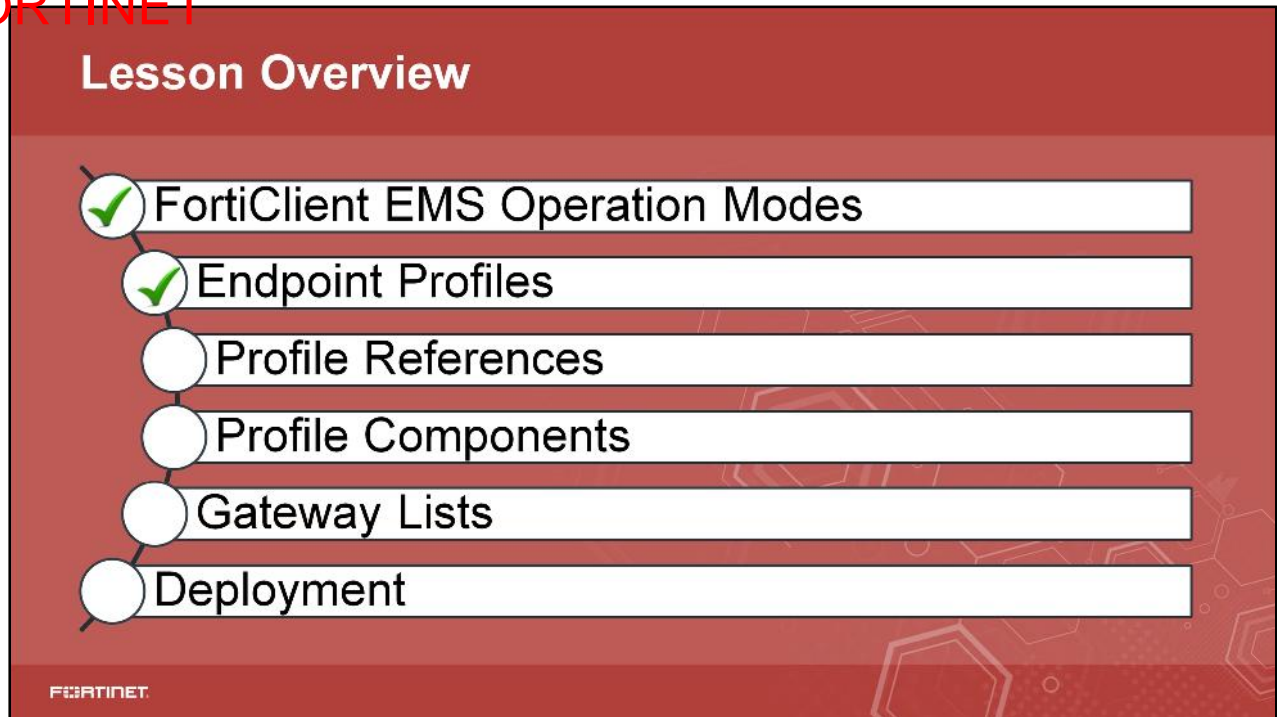
Deleting profiles: You can delete any newly created profile. But note that you cannot delete the default profile and *not* assigned profiles.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which endpoint profile is assigned to unassigned workgroups and domains
 - A. Custom endpoint profile
 - ✓ B. Default endpoint profile
2. To import a profile from FortiGate what must you open access to?
 - A. FTP
 - ✓ B. HTTPS

DO NOT REPRINT
© FORTINET



Good job! You now know how configure, edit, assign, and manage endpoint profiles.

Now, you will learn about endpoint references.

DO NOT REPRINT
© FORTINET

FortiClient EMS: Endpoint References

Objectives

- Configure endpoint references

FORTINET

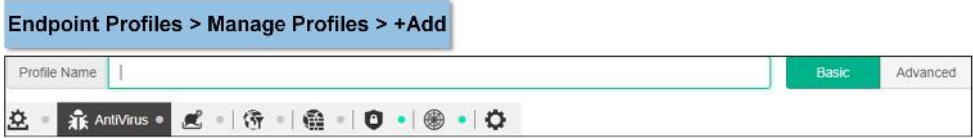
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring endpoint references, you will be able to implement the required settings to use endpoint references in your network.

DO NOT REPRINT
© FORTINET

Profile Name

- Only the Web Filter and System Settings tabs are available for Chromebooks
- You can give a name to a profile
- There are two display options for configuration
 - Basic
 - Advanced



Endpoint Profiles > Manage Profiles > +Add

Profile Name

Basic Advanced

AntiVirus

FORTINET

20


For Chromebooks, only the **Web Filter** and **System Settings** tabs are available. All other tabs are exclusive to Windows, macOS, and Linux endpoints.

Profile Name: Allows you to enter a name and select a display option. **Basic** shows all the GUI options. The **Advanced** display option enables the XML configuration tab to configure a profile using XML. This option is only available for Windows, macOS, and Linux profiles.

DO NOT REPRINT
© FORTINET

AntiVirus Protection

- AntiVirus tab enables antivirus protection
 - Real-Time Protection
 - On Demand Scanning
 - Scheduled Scan
 - Anti-Exploit
 - Removable Media Access
 - Exclusions
 - Other
- Sandbox tab enables sandbox detection
 - Server
 - File Submission Options
 - Remediation Actions
 - Exceptions


21

AntiVirus: Enables antivirus protection. Some options display only if you enable **Advanced**.

- **Real-Time Protection:** FortiClient can take different actions on virus discovery. It can block access to known communication channels and access to malicious websites. It also identifies malware and exploits using signatures received from FortiSandbox. This function is available only if the **Sandbox Detection** tab is available. You can also select file size and scan files accessed by a user or system process, such as Read or Write.
- **On Demand Scanning:** It integrates FortiClient into the Windows Explorer' Menu. You can enable to pause scanning when a computer is running on battery power, and automatically submit suspicious files to FortiGuard for analysis.
- **Scheduled Scan:** You can select schedule type, scan type, and priority. You can also select removable media and network drives for scanning.
- **Anti-Exploit:** Enables the anti-exploit engine to monitor commonly used applications for attempts to exploit known vulnerabilities. You can exclude applications from anti-exploit detection and enable system tray notifications.
- **Removable Media Access:** Enables controlling access to removable media devices.
- **Exclusions:** Enable exclusions from antivirus scanning.
- **Other:** Enables scan for rootkits, adware, riskware, email, media on insertion, and advanced heuristics signature.

Sandbox: Enables sandbox detection. Some options display only if you enable **Advanced**.

- **Server:** Allow to select FortiSandbox in the network. You can select file access options based on results.
- **File Submission Options:** You can select file resources like removable media, network drives, web downloads, and email downloads.
- **Remediation Actions:** Select **Quarantine** or **Alert & Notify** for infected files.
- **Exceptions:** You can exclude files from trusted sources and specific files or folders.

DO NOT REPRINT
© FORTINET

Web Filter

- You must enable FortiProxy to use web filter options
- Web Filter:
 - Enables **Client Web Filtering When On-Net**
 - You can select site categories from FortiGuard
 - You can select actions for entire site categories and subcategories

Local Profiles > (Profiles Name) > Web Filter

Web Filter ☒

General

☒ Client Web Filtering When On-Net

☐ Log All URLs

☐ Log User Initiated Traffic

☐ Show Bubble Notification When HTTPS Site Is Blocked

Site Categories

		Adult/Mature Content
		Bandwidth Consuming
		General Interest - Business
		General Interest - Personal
		Potentially Liable
		Security Risk
		Unrated

☐ Rate IP Addresses

☐ Allow websites when rating error occurs

Exclusion List

Save **Discard Changes**

FORTINET

22

Web Filter: Enables web filtering options. For Windows, macOS, and Linux profiles, you must enable **FortiProxy (Disable Only When Troubleshooting)** on the **System Settings** tab to use the **Web Filter** options.

General:

- Client Web Filtering When On-Net:** FortiClient does web filtering even when it's On-net with FortiGate in the network also configured with web filter profile. This is only available for Windows and macOS profiles. This setting affects the **Block Access to Malicious Websites** setting in AntiVirus protection.
- Log All URLs:** Enables logging for all URLs.
- Log User Initiated Traffic:** Includes user information in web filtering logs.
- Show Bubble Notification When HTTPS Site Is Blocked:** Enables the showing of a bubble notification when HTTPS site is blocked
- Save Search:** You can enable safe search option for search engines like Google search or YouTube.

Site Categories: Enables site categories from FortiGuard. When site categories are disabled, FortiClient is protected by the exclusion list. For all categories below, you can configure an action for the entire site category by selecting either **Block**, **Warn**, **Allow**, or **Monitor**. Each site category is listed below:

- Adult/Mature Content
- Bandwidth Consuming
- General Interest-Business
- General Interest-Personal
- Potentially Liable
- Security Risk
- Unrated

DO NOT REPRINT
© FORTINET

Web Filter (Contd)

- Filter URL and resolve IP address at the same time
- Create exclusion list with action:
 - Allow
 - Block
 - Monitor
- FortiClient is protected by the exclusion list when no site categories enabled

Local Profiles > (Profiles Name) > Web Filter

☒ Rate IP Addresses ⓘ

☐ Allow websites when rating error occurs

Exclusion List ⓘ

Simple Perform a case-insensitive matching against URLs.

Wildcard `?` matches any character once. For example, the pattern `123???` will match `123a` or `123abc`, but not `123abcdef`. `*` matches zero or more characters.

Regular Expression Use Perl Compatible Regular Expressions (PCRE) to perform matching against URLs.

☐ `www.facebook.*`

FORTINET

23

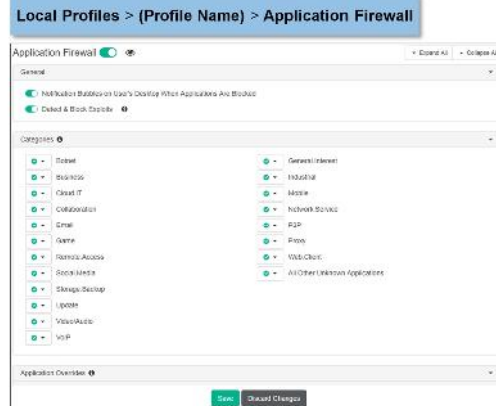
Rate IP Addresses: You can also filter URLs and resolved IP addresses at the same time and select the action for rating errors.

Note that if the **Allow websites when rating error occurs** option is enabled, FortiClient will block all URLs, including the captive-portal authentication page. This will prevent users from getting access to the authentication page.

Exclusion List: You can select an action, and enter specific URLs and their type, such as simple, wildcard, or regular expression.

Application Firewall

- The **Application Firewall** tab enables application control on endpoint
 - Enables notification when applications block
 - Inspect network traffic for intrusions
 - Enables FortiClient firewall to allow, block, or monitor applications
 - Use signatures to identify applications
 - Applications divide into category



FORTINET

24

Application Firewall: Use this switch to enable or disable application control.

- **General:** You can enable bubble notifications for block applications. You can also enable to inspect network traffic for intrusions attempting to exploit known vulnerabilities.
- **Categories:** You can take different actions on these categories:
 - Botnet, Business
 - Cloud.IT, Collaboration
 - Email
 - Game, General.Interest
 - Industrial
 - Mobile, Network.Service
 - P2P, Proxy
 - Remote.Access
 - Social.Media, Storage.Backup
 - Update
 - Video/Audio, VoIP
 - Web.Others
 - All Other Unknown Applications
- **Application Overrides:** Enable FortiClient firewall to *allow*, *block*, or *monitor* applications based on their signature. You can delete an application and add a signature to an application.

DO NOT REPRINT
© FORTINET

VPN

- Enables VPN provisioning
- Support IPsec and SSL VPN
- Allows user to add VPN tunnels
- Disable option to connect/disconnect
- You can enable SSL VPN DNS cache server control
- IPsec can use Windows Store Certificates
- Configure basic and advance VPN settings

Local Profiles > (Profile Name) > VPN

FORTINET

25

Use the settings on the **VPN** tab enable or disable VPN use on endpoints. There are general and specific VPN type settings available to configure.

General: You can enable or disable **Allow Personal VPN**, **Disable Connect/Disconnect**, **Show VPN before Logon**, **Minimize FortiClient Console on Connect**, **Show Connection Progress**, **Use Vendor ID** and **Current Connection**. You can also select a maximum number of attempts.

SSL VPN: The options in the **DNS Cache Service Control** are:

- **Disable dnscache service**
- **Leave dnscache service unchanged**
- **Restart dnscache service**
- **Restart dnscache service with SC command**

You can also override DNS server to SSL VPN DNS IP.

IPsec VPN: Enable or disable the following:

- **Beep If Connection Fails**
- **Use Windows Store Certificates**
- **Current User Windows Store Certificates (IPsec only)**
- **Local Computer Windows Store Certificates (IPsec only)**
- **Use Smart Card Certificates**
- **Show Auth Certificates Only**
- **Block IPv6**
- **Enable UDP Checksum**
- **Disable Default Route**
- **Check for Certificate Private Key**
- **Enhanced Key Usage Mandatory**

DO NOT REPRINT
© FORTINET

VPN

- VPN Tunnels
 - You can add IPsec or SSL VPN profiles
 - There are basic and advanced settings
- SSL VPN
 - You can add multiple remote gateway IPs
 - Default access port is 443
 - Select certificate for additional security
 - On connect and on disconnect script
- IPsec VPN
 - You can add multiple remote gateway IPs
 - Authentication method
 - VPN settings
 - Phase1 and 2 settings
 - On connect and on disconnect script

VPN > +Add Tunnel > SSL VPN

VPN > +Add Tunnel > an IPsec VPN

28

You can add VPN profiles both SSL and IPsec.

SSL VPN: The SSL settings includes remote gateway IP, SSL port number, an options to request the certificate and prompt for user name. There is also option to enter connect and disconnect scripts, which also an needs to be enabled on the FortiGate.

IPsec VPN: The following options are available when you select IPsec VPN:

- **General:** It includes remote gateway IP, authentication method, pre-shared key (if **Pre-Shared Key** is selected for **Authentication Method**) and prompt username.
- **VPN Settings:** It includes the following:
 - IPsec mode: Select **Main** or **Aggressive**
 - Options: Select **Mode Config**, **Manual Set**, or **DHCP over IPsec**.
 - DNS Server: Specify DND server for the VPN tunnel if **Manual Set** is selected.
 - Assign IP Address: Enter IP address to assign to tunnel. Available for **Manual Set**.
 - Split Table: Enter IP address and subnet mask for the VPN tunnel. Available for **Manual Set** or **DHCP over IPsec**.
- **Phase 1:** Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
- **Phase 2:** Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals that you specify must match the configuration on the remote peer.

FortiClient 6.0 Study Guide

182

Vulnerability Scan

- **Vulnerability Scan** tab enables scan on endpoints

- Scanning on connecting to FortiGate
- Scan for OS and vulnerability signature updates
- Configure automatic maintenance
- Configure scheduled scans
- Configure automatic patching
- Create exclusion list

Local Profiles > (Profile Name) > Vulnerability Scan

The screenshot displays the 'Vulnerability Scan' configuration page in the FortiClient EMS. The page is organized into several sections:

- Scanning:** Includes checkboxes for 'Scan on Registration', 'Scan on Vulnerability Signature Update', 'Scan for OS updates', and 'Enable Proxy'.
- Automatic Maintenance:** Features a toggle for 'Automatic Maintenance' and a 'Schedule' section with options for 'Type' (Daily, Weekly, Monthly) and 'Scan On' (Day of the week).
- Automatic Patching:** Includes a toggle for 'Automatic Patching' and a 'Severity' dropdown menu.
- Exclusions:** Contains a list of applications that can be excluded from scanning, with columns for application name and a checkbox for exclusion.

FORTINET

27

Scanning:

- **Scan on Registration:** Scan endpoints upon connecting to a FortiGate.
- **Scan on Vulnerability Signature Update:** Scan endpoints upon updating a vulnerability signature.
- **Scan for OS:** Updates scan for OS updates.
- **Enable Proxy:** Enable proxy.

Automatic Maintenance: Configure settings for automatic maintenance. This configures the vulnerability scan to run as part of Windows automatic maintenance. Adding FortiClient vulnerability scans to the Windows automatic maintenance queue allows the system to choose an appropriate time for the scan.

Scheduled Scan: Configure settings for scheduled scanning. In the **Schedule Type** drop-down list you can select **Daily**, **Weekly**, or **Monthly**. In the **Scan On** field, you can configure the day the scan will run. This setting applies if the schedule is *Monthly*. You can also specify the time the scan will start.

Automatic Patching: When enabled, patches are installed automatically when vulnerabilities are detected. Select one of the following:

- **Critical:** Patch critical vulnerabilities only.
- **High:** Patch high severity, and above, vulnerabilities.
- **Medium:** Patch medium severity, and above, vulnerabilities.
- **Low:** Patch low severity, and above, vulnerabilities.
- **All:** Patch all vulnerabilities.

Exclusions:

- **Exempt Application Vulnerabilities Requiring Manual Update from Vulnerability Compliance Check.** This option does not exclude applications from vulnerability scanning.
- **Exclude Selected Applications from Vulnerability Compliance Check**

System Settings

- **System Settings** tab enables to set:
 - How the FortiClient user interface appears
 - It includes:
 - Dashboard banner
 - Lock password
 - Backing up FortiClient configuration
 - Hide system tray
 - Language
 - Specify log FortiClient log settings
 - Select log level
 - Select feature for which logs will be generated
 - Proxy
 - Use proxy server for FortiGuard updates and virus submission

FORTINET

The majority of these configuration options are only available for Windows, macOS, and Linux profiles. Some options are available for Chromebook profiles, such as **Upload Logs to FortiAnalyzer/FortiManager**. Some options are available only when **Advanced** view is enabled.

UI: Specifies how the FortiClient user interface appears when installed on endpoints.

Log: Specifies log settings such as **Level** and **Features** for which logs will generate:

- **Disabled**
- **Emergency:** The system becomes unstable.
- **Alert:** Immediate action is required.
- **Critical:** Functionality is affected.
- **Error:** An error condition exists and functionality could be affected.
- **Warning:** Functionality could be affected.
- **Notice:** Information about normal events.
- **Info:** General information about system operations.
- **Debug:** Debug FortiClient.

You can also select **Client-Based Logging When On-Net** and **Upload Logs to FortiAnalyzer/FortiManager**.

Proxy: Enable to access FortiGuard and submit virus to FortiGuard using the configured proxy. You can select proxy type, IP, port, username, and password.

DO NOT REPRINT
© FORTINET

System Settings

- **Update**
 - Specify to use FortiManager or Micro-FortiGuard server for updates
 - Enables FortiClient software update
 - Select update action, scheduling, and server location
- **FortiProxy**
 - You must enable **FortiProxy** to use the Web Filter options as well as some AntiVirus options
 - Enables **HTTPS Proxy** to inspect https traffic
 - Email server and client comforting
- **Endpoint Control**
 - Specify settings for endpoints
 - You can enable
 - Show Bubble Notifications
 - Silent registration
 - On-Net Subnets

Local Profiles > (Profile Name) > System Settings

Update

☐ Use FortiManager for updates (requires license)

☒ Software update

☒ Scheduled update

Update type:

Update interval: hours

FortiGuard server location:

FortiProxy

☒ FortiProxy (Disable Only When Troubleshooting)

☒ HTTP Proxy

HTTP Timeout: seconds

☒ HTTPS Client Comforting

☒ POP3 Server Comforting

☒ SMTP Client Comforting

☒ Web Filter

URL Filter:

Endpoint Control

☒ Show Bubble Notifications

☒ Silent registration

☒ Log off When User Logs Out of Windows

☐ Disable Unregister

☐ Hide Compliance Enforcement Feature Message from Compliance Tab

☐ On-Net Subnets

Save Cancel

FORTINET

29

Update: You can specify to use FortiManager or Micro-FortiGuard Server for FortiClient updates. You can also select FortiClient software updates, the update schedule, and FortiGuard server location.

FortiProxy: Enable **FortiProxy (disable only when troubleshooting)**. You must enable FortiProxy to use the Web Filter options as well as some AntiVirus options. You can enable **HTTPS Proxy**. If disabled, FortiProxy no longer inspects HTTPS traffic. It also enables **HTTP Timeout**, **POP3 Client Comforting**, **POP3 Server Comforting**, **SMTP Client Comforting**.


Endpoint Control: Specify the settings for endpoint such as:

- **Show Bubble Notifications**
- **Show Profile Details**
- **Silent Registration**
- **Log off When User Logs Out of Windows**
- **Disable Unregister**
- **Hide Compliance Enforcement Feature Message from Compliance Tab**
- **On-Net Subnets**

DO NOT REPRINT
© FORTINET

System Settings and XML

- Other
 - Enable to select and install a CA certificate on endpoints
 - Select to enable single sign-on (SSO) mobility agent
- iOS
 - Enable and browse for `.mobileconfig` file to distribute the configuration profile
- Privacy
 - Send usage statistics to Fortinet to improve product
- XML Configuration
 - Use XML editor to configure FortiClient settings

30

Other: Enable to install CA certificate on client, you can add certificates by clicking **Profile Components > Manage CA Certificates**. It also enables SSO mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device.

iOS: Select this to enable and browse for your `.mobileconfig` file to distribute the configuration profile.

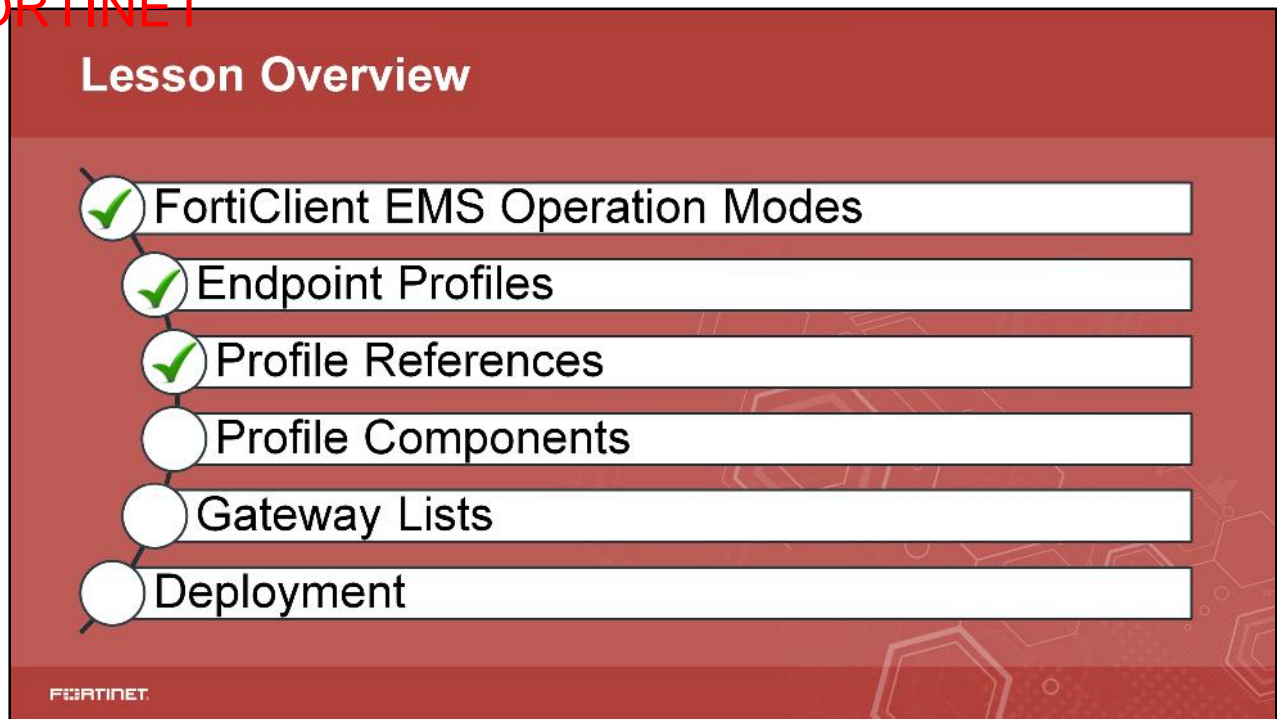
XML Configuration: Use XML editor to configure FortiClient options and settings.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which feature tabs are available for Chromebooks?
 - ✓ A. **WebFilter** and **System Settings**
 - B. **WebFilter, Application Firewall, and VPN**
2. Which of these features FortiProxy?
 - A. Application Firewall
 - ✓ B. **WebFilter**

DO NOT REPRINT
© FORTINET



Good job! You now understand how to use endpoint references.

Now, you will learn about profile components.

DO NOT REPRINT
© FORTINET

Profile Components

Objectives

- Manage FortiClient installers
- Manage FortiSandbox
- Manage certificates

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in working with profile components, you will be able to manage installers, FortiSandbox, and certificates.

DO NOT REPRINT
© FORTINET

Managing Installers

- FortiGuard Distribution Network
 - FortiClient EMS automatically connects to FortiGuard Distribution Network (FDN)
 - To provide access to FortiClient installers you can use with FortiClient EMS profiles.
 - Download manually if no connection to FDN
 - You can download installer to use from these locations:
 - <https://support.fortinet.com>
- Creating FortiClient installers
 - You can specify what FortiClient features to include
 - Feature can include and then disable to use later
 - Installers for Windows OS and macOS add to FortiClient
 - EMS

Profile Components > Manage Installers > +Add

FORTINET

34

FortiClient EMS automatically connects to FDN to provide access to FortiClient installers that you can use with FortiClient EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS.

You can download FortiClient installers to use with FortiClient EMS from the following locations:

- <https://support.fortinet.com>

You can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint. When you create a FortiClient installer in FortiClient EMS, an installer for the Windows operating system and an installer for the macOS operating system are added to FortiClient EMS. You can also select **Advanced Options** such as automatic registration, desktop shortcut, start menu and endpoint tag.

Fortinet does not recommend to install webfilter and application firewall features on Windows server OS.

Note that after you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

DO NOT REPRINT
© FORTINET

Managing Installers

- Uploading custom FortiClient installers
 - You can create a custom installer and add to FortiClient EMS
 - Manually download and add to EMS if no connection to FDN
 - Option to select Windows or Mac OS installer
 - Supports both 64-bit and 32-bit
 - Configure endpoint tag, EMS, and FortiGate details

Profile Components > Manage Installers > +Add

FORTINET

35

You can create a custom FortiClient installer and add it to FortiClient EMS. Alternately, if a connection to FDN is not available, you may need to manually download a FortiClient installer and add it to FortiClient EMS. Select **Upload** in **Add Installer** dialog box in the **Version** list.

There are options to select Windows or MacOS and 64-bit or 32-bit installer for Windows OS. In the **Advanced** tab, you also select endpoint tag, EMS, and FortiGate. For FortiGate and endpoint tag, a gateway list and endpoint tag must have configured.

The online installer available for download at `FortiClient.com` cannot be uploaded into the **Add Installer** dialog in **Manage Installers**.

Managing Installers

- You can view on the Manage Installers pane after you add them on EMS
- Profile Components > Manage Installers displays:
 - Available Installer
 - View Details
 - Turn on/off Auto Update
 - Add
 - Refresh
- You can delete an installer by selecting it and clicking Delete

Profile Components > Manage Installers

OS	Version	Auto Update	Name	Location
OS	6.0.3	Enabled	FortiClient Version 6	https://39.91.188.18440/installers/FortiClient-version-6/
OS	MAC OS X, Windows			
Version	6.0.3			
Features	Antivirus, Application Firewall, Secure Access Architecture Components, Security Fabric Agent, VPN Filtering			
Managed by EMS	Provisioned with BOTS			
Auto Update	Disabled			
Desktop Shortcut	Enabled			
Start Menu Shortcut	Enabled			
Notes	6.0.3 install			

FORTINET

35

After you add FortiClient installers to FortiClient EMS, you can view them on the **Manage Installers** pane. The **Manage Installers** displays the available installer list, name of installer, OS, FortiClient version, enabled features and other related information about installer.

You can also enable or disable auto update. When auto update is enabled, FortiClient EMS automatically keeps the installer updated to the latest patch.

To delete a FortiClient installer, do the following:

- Click **Profile Components > Manage Installers**.
- Click the desired installer, then click **Delete**.
A confirmation dialog box opens.
- Click **Yes**.
The FortiClient installer is deleted from FortiClient EMS.

Managing FortiSandbox Units

- You can add, view, and edit FortiSandbox units on the **Manage FortiSandboxes** pane
- Configure a synchronization schedule between EMS and FortiSandbox
- FortiClient EMS detects FortiSandbox units from the **Sandbox Detection** tab
- You can also delete FortiSandbox unit(s) on **Manage FortiSandboxes** pane

Profile Components > Manage FortiSandboxes > +Add

FortiSandbox

FortiSandbox name: Required

IP address/hostname: Required

Scheduled synchronization: sync 2019-02-08 00:00 every 1 hour(s)

Inspection mode: None All High-Risk Ext. Custom

Before EMS removes the list of supported extensions from FSA, **Custom** mode is not available. **All High-Risk Ext.** mode may list the extensions that are not supported by the FSA.

Name	Address	Inspection M...	Status	Last Synced	Next Sync
test	172.17.60.138	All High-Risk	Authorization: Not Author... Extension list: Synchronized	2018-07-08 1...	2018-07-08 1...

FORTINET

37

On the **Manage FortiSandboxes** pane, you can add, view, and edit FortiSandbox units, including configuring the synchronization schedule between FortiClient EMS and FortiSandbox. FortiSandbox units configured on the **Manage FortiSandboxes** pane can be selected from the **Sandbox Detection** tab when creating or editing an endpoint profile.

To delete a FortiSandbox device, do the following:

1. Click **Profile Components > Manage FortiSandboxes**.
2. Select the desired FortiSandbox.
3. Click **Delete**.
4. Click **Yes**.

Note that you can delete the profile only if it is not assigned to or used in an endpoint profile.

DO NOT REPRINT
© FORTINET

Managing CA Certificates

- You can upload or import CA certificate into FortiClient EMS
- You can upload locally by browsing the file
- Importing certificate from FortiGate requires
 - FortiGate IP address
 - VDOM
 - Login username
 - Login password

Profile Components > Manage CA Certificates > Upload

Upload Local Certificate

Browse...

Profile Components > Manage CA Certificates > Import

Import Certificates from FortiGate

IP address/hostname

VDOM

Username

Password

30

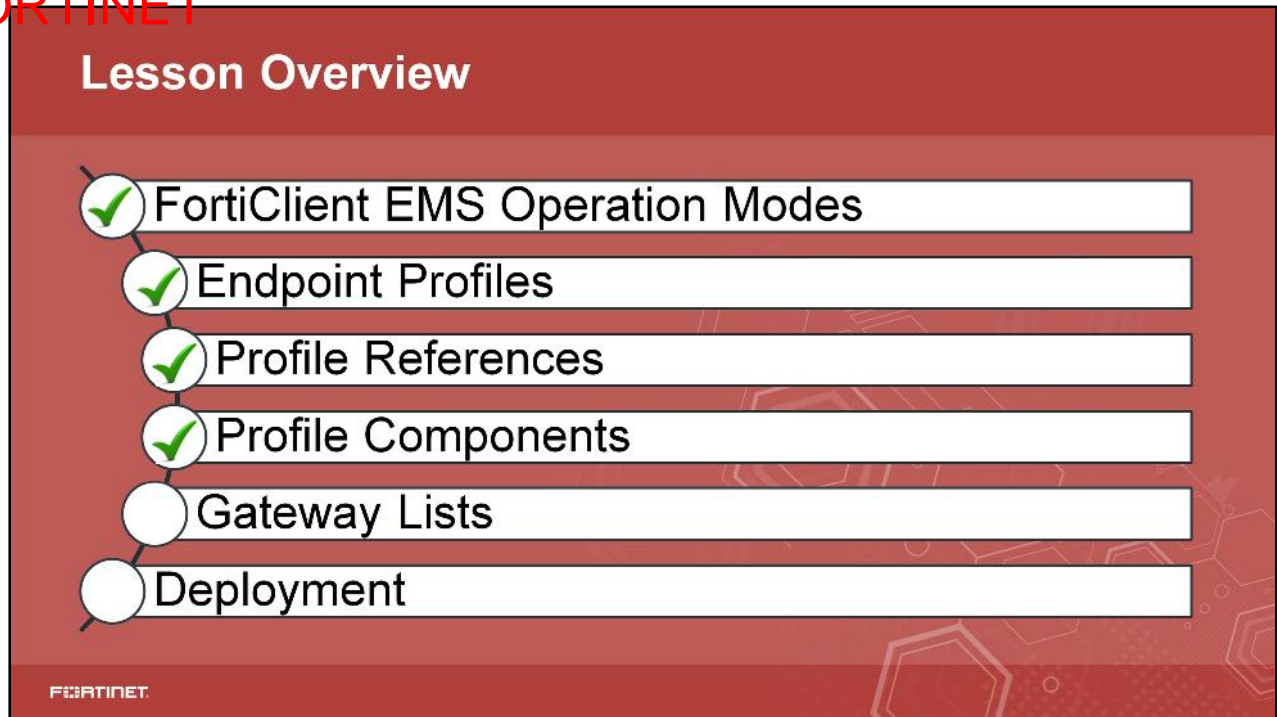
You can upload or import CA certificates into FortiClient EMS. You can upload CA certificates locally. To import a certificate from FortiGate, you need FortiGate's login details.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. By what method can you add a custom installer to FortiClient EMS?
 - A. Connection to FDS
 - ✓ B. Manual upload
2. Which of the following is required to import a certificate from FortiGate?
 - A. FortiGate configuration file
 - ✓ B. FortiGate log in details

DO NOT REPRINT
© FORTINET



Good job! You now understand profile components.

Now, you will learn about gateway lists.

DO NOT REPRINT
© FORTINET

Gateway Lists

Objectives

- Create and view gateway lists
- Export gateway lists to XML

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in creating, viewing, and exporting gateway lists, you will be able to work with them in your network.

Manage Gateway Lists

- You can create a gateway list that contains multiple FortiGate IP addresses
- FortiClient search for IP address and connects
- IP address search moves from top to bottom
- After you create and save you can export gateway list in XML format

FORTINET

42

You can create a gateway list that contains IP addresses for multiple FortiGate devices. FortiClient searches for IP addresses in its subnet in the gateway IP list and connects to the FortiGate on the list that is in the same subnet as the host system. If FortiClient cannot find any FortiGate devices in its subnet, it attempts to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was configured in the gateway list. To add additional IP addresses, press Enter.

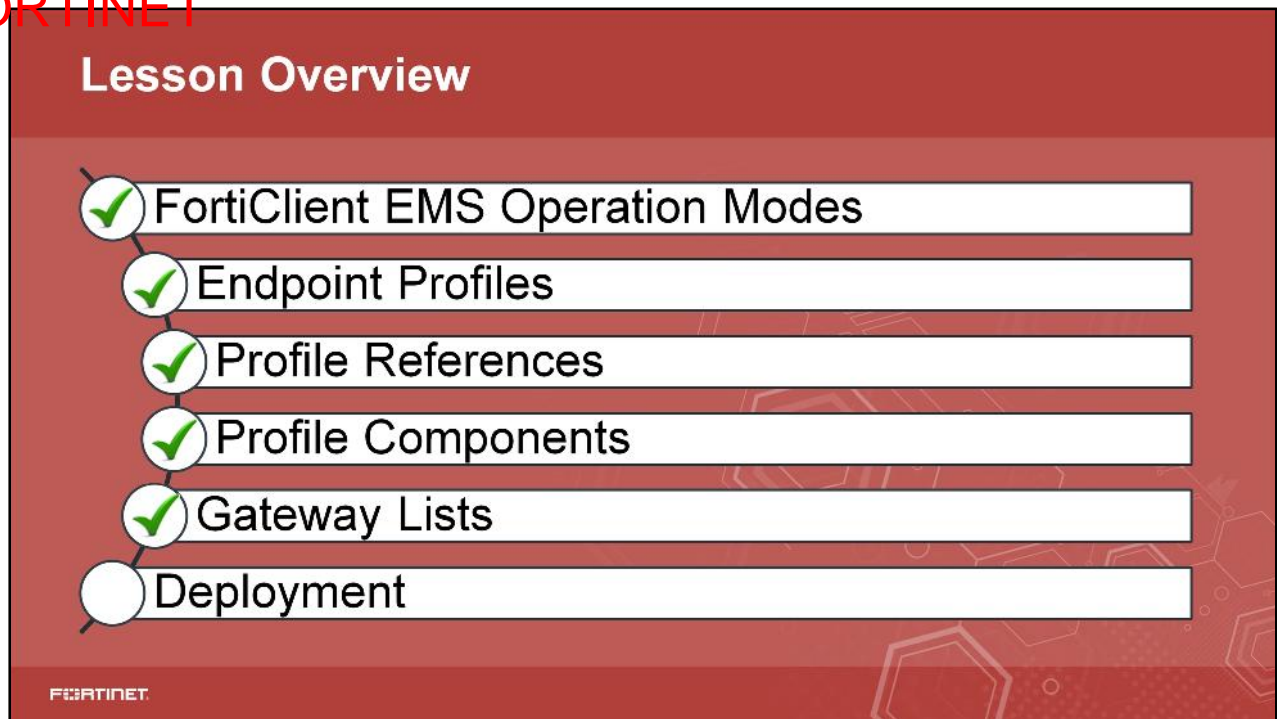
You need the following information to create a gateway list:

- **Name:** Enter the list name
- **Comment:** Enter additional comments (optional)
- **IP addresses/Hostnames:** Enter the IP address(es) or hostname(s) of the FortiGate devices. You can also use an FQDN. Press the **Enter** key to add additional IP addresses
- **Connect to local subnets only:** Enable to only allow connection to local subnets
- **Use connection key:** Enable the connection key endpoints can use to connect to FGT
- **New connection key:** Enter the connection key
- **Confirm new connection key:** Re-enter the connection key to confirm
- **Managed by EMS:** Select an option from the drop-down list. Users can configure this IP address in **System Settings > Server**

After you create and save a gateway list, the **Export XML** button displays, and you can export the list to a configuration file in XML format.

You can assign gateway lists to endpoints. When you assign the IP list and FortiClient Telemetry data connection process has started, the endpoint connects to a FortiGate or EMS, based on the gateway list. View lists by selecting an endpoint and then clicking **Summary > Configuration > Gateway List**.

DO NOT REPRINT
© FORTINET



Good job! You now understand gateway lists.

Now, you will learn about FortiClient deployment.

DO NOT REPRINT
© FORTINET

FortiClient EMS: Deployment

Objectives

- Prepare the AD server for deployment
- Prepare the Windows endpoint
- Understand deployment types

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient deployment, you will be able to prepare Windows AD server and endpoints, as well as implement different deployment types.

Prepare AD Server

- You must install and prepare the AD server before you deploy FortiClient installation
 - Configure a group policy under **Group policy Management**
 - Use **Default Domain Policy** or create new to assign to OU that contains endpoint
 - Configure Windows services in Group Policy Management editor
 - **Task Scheduler**: Automatic
 - **Windows Installer**: Manual
 - **Remote Registry**: Automatic
 - Configure deployment rules for Windows firewall
 - Allow inbound connection for SMB-In and RPC
 - Configure Windows firewall domain profile settings
 - Allow inbound file and printer sharing exception
 - Allow inbound remote administration exception
 - Allow **ICMP Exceptions** > **Allow inbound echo request**
- You cannot use workgroups and macOS to deploy an initial installation
- You can use FortiClient EMS to uninstall and update FortiClient on endpoints

To deploy FortiClient from FortiClient EMS, you must prepare the AD server for deployment and deploy FortiClient on the endpoints. Before you can successfully deploy a FortiClient installation, ensure you install and prepare the AD server as follows:

1. Configure a group policy on the AD server.

On the AD server open **Group policy Manager** and right-click the **Default Domain Policy** setting. The **Group Policy Management Editor** opens. A new policy is applied to the entire AD domain. Alternatively, you can create a new Group Policy Object, and link it to one or more organizational units (OU) in the AD server that contains the endpoint computers on which FortiClient will be deployed.

2. Configuring required Windows services.

Configure Windows services in **Computer Configuration > Policies > Windows > Settings > Security Settings > System Services** as mentioned in the slide.

3. Creating deployment rules for Windows firewall.

You need new inbound rules to allow **File and Printer Sharing(SMB-In)** and **Remote Scheduled Tasks Management (RPC)**.

4. Configure Windows firewall domain profile settings

You must add exceptions for domain profile

- **Allow inbound file and printer sharing**(require EMS server's IP address)
- **Allow inbound remote administration**(require EMS server's IP address)
- **Allow ICMP Exceptions > Allow inbound echo request**

Note that you cannot use FortiClient EMS to deploy an initial installation of FortiClient to endpoints (macOS and workgroup computers). However, after FortiClient is installed on endpoints and the endpoints are connected to FortiClient EMS, you can use FortiClient EMS to uninstall and update FortiClient on endpoints.

DO NOT REPRINT
© FORTINET

Prepare Windows Endpoints

- You must prepare the Windows endpoint before deploying FortiClient installation
 - Configure Windows services
 - **Task Scheduler:** Automatic
 - **Windows Installer:** Manual
 - **Remote Registry:** Automatic
 - Configure Windows firewall rules
 - Allow inbound connection for file and printer sharing (SMB-In)
 - Allow inbound connection for remote scheduled tasks management (RPC)
- AD administrator account use for AD group deployments
- An installer URL is shared for non-AD deployments
 - Who can download and install FortiClient manually

FORTINET

45

You must enable and configure the following services on each Windows endpoint before FortiClient deployment:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic

The Windows firewall must allow SMB-In and RPC traffic for inbound connections.

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in **Manage Installers**. Click **Profile Components > Manage Installers**.

Note that when you are adding endpoints using an AD domain server, FortiClient EMS automatically resolves endpoint IP addresses during initial deployment of FortiClient. FortiClient EMS can deploy FortiClient (Windows) to AD endpoints that do not have FortiClient installed, as well as upgrade existing FortiClient installations if the endpoints are already connected to the EMS server.

You can execute `gpresult.exe /H gpresult.html` on any AD client to verify if you have an issue pushing the group policy to the endpoints.

Deploying FortiClient

- Deploy a FortiClient installation from FortiClient EMS using an AD server
 - Add the AD server to FortiClient EMS by adding a domain
 - Add a FortiClient installer package to FortiClient EMS
 - Add a profile
 - Select the FortiClient installer package
 - Configure FortiClient features in the profile
 - Assign the profile to the AD domain to push the FortiClient installation process on the endpoints
 - Verify the deployment by monitoring FortiClient connections to the FortiClient EMS
- Deploying initial installations of FortiClient (macOS)
 - Create a custom FortiClient (macOS) installer on FortiClient EMS and send the installer download link to users so they can install FortiClient manually
 - Use a third-party application to perform initial deployment of FortiClient (macOS) to endpoints
- Deploying FortiClient upgrades from EMS
 - You can deploy a FortiClient software update from EMS
 - Prompt appears on endpoint when installer package to be deployed

Deploying FortiClient on endpoints: For successful deployment of FortiClient installation from FortiClient EMS using AD server, you must prepare the AD server, add the AD server to FortiClient EMS as a domain, add an installer package to FortiClient EMS, add a profile, which includes the installer package and configured FortiClient features, and assign the profile to a branch of the AD domain to push the installation. You can verify the deployment by monitoring FortiClient connections to the EMS.

Deploying initial installations of FortiClient (macOS): FortiClient EMS cannot be used to deploy initial installations of FortiClient (macOS). You can deploy an initial installation of FortiClient (macOS) by doing one of the following:

- Create a custom FortiClient (macOS) installer on EMS with the EMS IP address embedded. Send the installer download link to users so they can install FortiClient manually on the endpoint.
- Use a third-party application to perform the initial deployment of FortiClient (macOS) to endpoints.

After FortiClient (macOS) is installed on endpoints and you have connected FortiClient Telemetry to FortiClient EMS, you can use FortiClient EMS to replace, upgrade, and uninstall FortiClient.

Deploying FortiClient upgrades from EMS: You can deploy a FortiClient software update from EMS. A prompt appears on the FortiClient endpoint when an installer package is requested to be deployed. The prompt requests the user to do one of the following:

- **Upgrade Now:** If this option is selected, it performs the upgrade and automatically restarts your computer.
- **Upgrade Later:** If this option is selected, you can indicate the time to start the upgrade. The default is 8:00 PM. Your computer automatically restarts after the upgrade.

If no option is selected, the upgrade occurs by default at 8:00 PM. After FortiClient EMS uninstalls the previous version, it asks if the user wants to **Reboot now** or **Reboot later**.

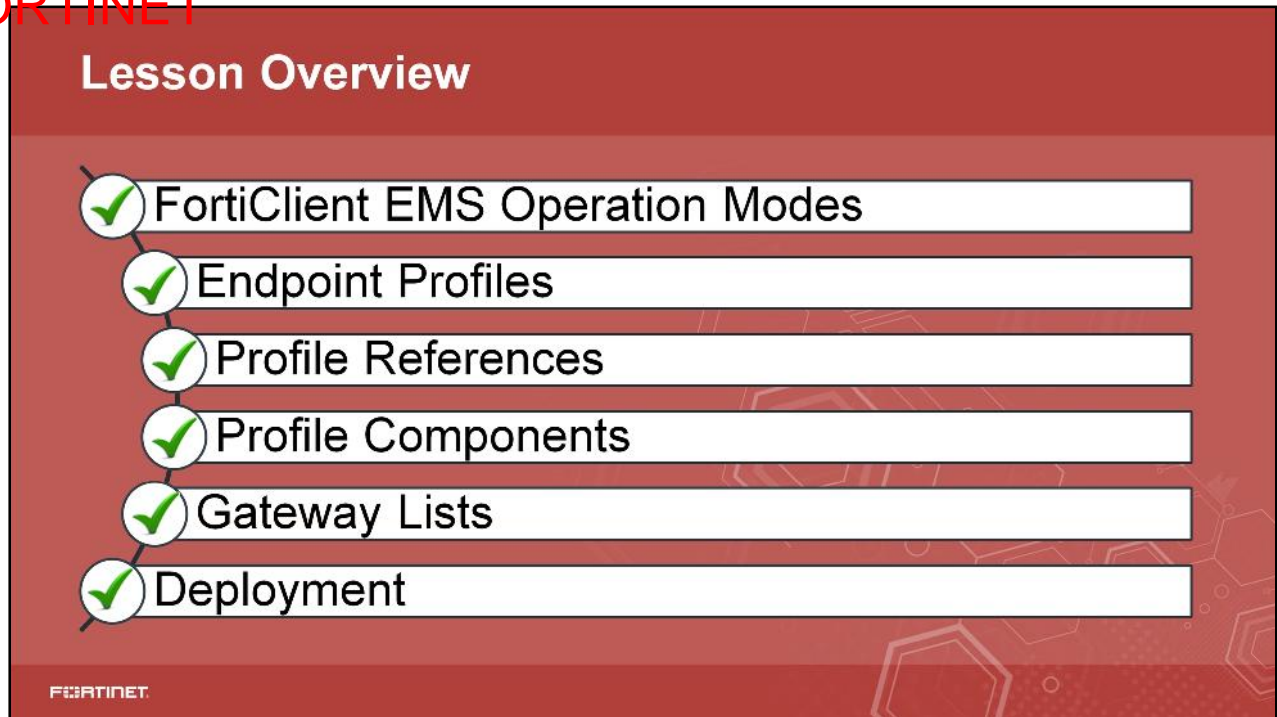
DO NOT REPRINT
© FORTINET

Knowledge Check

1. What Windows services are required on the server and the client?
 - ✓ A. Remote Registry and Task Manager
 - B. Remote Access and FortiClient Proxy Service

2. Which of the following you can use to deploy the initial FortiClient installation?
 - ✓ A. Domain
 - B. Workgroup

DO NOT REPRINT
© FORTINET





Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

Review

- ✓ FortiClient EMS Operation Modes
- ✓ Endpoint Profiles
- ✓ Profile References
- ✓ Profile Components
- ✓ Gateway Lists
- ✓ Deployment



This slide shows the objectives that you covered in this lesson.


By mastering the objectives covered in this lesson, you learned how to use FortiClient EMS operation modes, endpoint profiles, profile references, and components. You also learned about deployment types and gateway list.

DO NOT REPRINT
© FORTINET



In this lesson, you will learn how to diagnose and troubleshoot FortiClient and FortiClient EMS issues.

DO NOT REPRINT
© FORTINET



Lesson Overview

- How to Approach FortiClient Issues
- Common Issues with FortiGate and EMS
- FortiClient Troubleshooting
- FortiClient EMS Troubleshooting
- FortiClient Features Troubleshooting

FORTINET

In this lesson, you will learn about the topics shown on this slide.

Approaching FortiClient Issues

Objectives

- Approach and troubleshoot FortiClient and FortiClient EMS issues

FORTINET

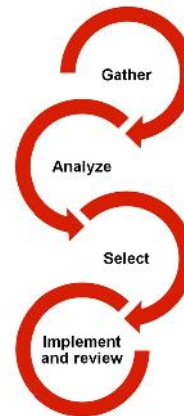
After completing this section, you should be able to approach and troubleshoot FortiClient and FortiClient EMS issues.

By demonstrating competence in approaching FortiClient issues, you will be able to solve FortiClient and FortiClient issues.

DO NOT REPRINT
© FORTINET

Approaching FortiClient Issues—Methodology

- Gather information to dissect problem
 - FortiClient version
 - Standalone or managed
 - Check minimum system requirements
 - Conflicting software—third-party antivirus software
 - New installation causing issues?
 - Did it ever work?
 - Existing installation—possible interference?
 - Was it working fine before?
 - Any changes to workstation or mobile device?
 - Any changes to FortiClient configuration?
 - Network changes
 - Connecting location



FORTINET

4

Before you can resolve a FortiClient issues, you need to identify the issue by gathering information to pinpoint and define it.

For example, if the issue is *registering FortiClient to FortiGate or FortiClient EMS*, check the following:
Has the registration process ever worked. Is the existing installation not working?

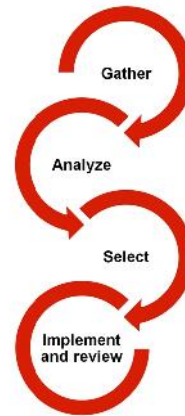
If yes, check for possible changes, such as changes to the device (OS updates, changes to administrator permissions), connection location (working from the office but not from home), and configuration and network changes.

Now you know the exact nature of the problem: *FortiClient is not registering from home*. The next step is to analyze the problem, which leads to possible opportunities to resolve the issue.

DO NOT REPRINT
© FORTINET

Approaching FortiClient Issues—Methodology (Contd)

- Analysis
 - Test on different workstation or mobile device
 - Other users having similar problems
 - Expected behaviour
 - Different behaviour
 - Reproducibility—always, random, unable to duplicate
- Possible solutions
 - List all possible options
 - Evaluate options in lab
 - Document
 - Implementation plan
 - Back out plan
- Implement and review the results
 - Monitoring and evaluation



FORTINET

5

The analysis phase requires testing, checking, and comparing with other users to find if they are encountering similar issues.

Once that is determined, to further dissect the issue, compare the expected results with your results and find out if the issue is reproducible, which results in a list of possible solutions to evaluate in the lab.

Remember, there might be multiple ways to resolve a issue. You should always document each of them and create a back up plan before implementing a solution in case you need to revert to a previous state.

Once you implement a solution, monitor and review the solution.

DO NOT REPRINT
© FORTINET

Lesson Overview

- ✓ How to Approach FortiClient Issues
- Common Issues with FortiGate and EMS
- FortiClient Troubleshooting
- FortiClient EMS Troubleshooting
- FortiClient Features Troubleshooting

FORTINET

Good job! You now understand how to approach FortiClient and FortiClient EMS issues.

Now, you will learn about FortiClient EMS issues.

FortiGate and EMS Issues

Objectives

- Understand diagnostic steps to resolve issues between:
 - FortiClient and EMS
 - FortiClient and FortiGate
 - How FortiClient determines on-net, off-net, and offline status

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in taking diagnostic steps, you will be able to diagnose and resolve common issues between FortiClient, FortiClient EMS, and FortiGate.

DO NOT REPRINT
© FORTINET

FortiClient Registration

- Registration methods—manual and automatic
- Manually entering FortiGate or EMS IP
- Automatic—four ways of automatic registration:
 - Telemetry gateway IP list
 - Connecting to the default gateway IP address (FortiGate IP)
 - Registration over VPN (if configured on FortiGate)
 - Remembered FortiGate

FORTINET

FortiClient uses the following methods in the following order to locate FortiGate or EMS for a telemetry connection:

- Manually entering the gateway IP address. The user enters the gateway IP address of FortiGate or EMS on FortiClient
- Telemetry gateway IP list: FortiClient Telemetry searches for IP addresses in its subnet in the gateway IP list. It connects to the FortiGate in the list that is also in the same subnet as the host system. If FortiClient cannot find any FortiGate devices in its subnet, it attempts to connect to the first reachable FortiGate on the list, starting from the top. The order of the list is maintained as configured on the gateway IP list.
- Default gateway IP address: The default gateway IP address is specified on the FortiClient endpoint and is used to automatically connect to FortiGate. This method does not support connections to EMS. FortiClient obtains the default gateway IP address from the operating system on the endpoint. The default gateway IP address of the endpoint should be the IP address of the FortiGate interface that has telemetry enabled.
- VPN
- Remembered gateway IP list: You can configure FortiClient to remember gateway IP addresses when you connect Telemetry to FortiGate or EMS. Later, FortiClient can use the remembered IP addresses to automatically connect Telemetry to FortiGate or EMS.

Note that FortiClient uses the same process to connect Telemetry to FortiGate or EMS after the FortiClient endpoint reboots, rejoins the network, or encounters a network change.

- Registration issues
 - IP and listening port on FortiGate or FortiClient EMS
 - Interface setting on FortiGate
- FortiClient logs
 - **Settings > Logging > Export logs**
- FortiGate CLI commands:
 - `diagnose endpoint record-list <ipv4-add`

```

3:41:39 PM Debug ESMAC [EPMONITORING] ESMAC_STATUS_REC_TO_IP
3:41:39 PM Debug ESMAC [EPMONITORING] ESMAC_STATUS_REC_TO_IP
3:41:39 PM Debug ESMAC [EPMONITORING] UserStart time
3:41:39 PM Debug ESMAC [EPMONITORING] Start searching for FGT
3:41:39 PM Debug Scheduler [EPMONITORING] handle processmanagement() called
3:41:39 PM Debug ESMAC [EPMONITORING] ESMAC_STATUS_REC_TERMINATES normally
3:41:39 PM Debug ESMAC [EPMONITORING] Timeout in select in SocketConnect
3:41:39 PM Debug ESMAC [EPMONITORING] Socket connect failed
3:41:39 PM Debug ESMAC [EPMONITORING] mSocketRecv, Secondary - 0
3:41:39 PM Debug ESMAC [EPMONITORING] ESMAC ConnectToSetState
3:41:39 PM Debug ESMAC [EPMONITORING] Not Registered
3:41:39 PM Debug ESMAC [EPMONITORING] mSubConnectionClientName false
3:41:39 PM Debug ESMAC [EPMONITORING] ESMAC ConnectToSetState
3:41:39 PM Debug ESMAC [EPMONITORING] Certificate not found
3:41:39 PM Debug ESMAC [EPMONITORING] The state has changed

```

```
FUNTIME0000090612 : diagnose endpoint resources-list  
second {}  
  
[IP address = 10.0.0.1]  
MAC address: 08:00:C9:7A:F0:0E  
Host MAC Address: 08:00:C9:7A:F0:0E  
MAC List = [08:00:C9:7A:F0:0E-A3]  
VCON = root  
EM online: yes  
EM address: 10.0.0.1100  
EM serial number: KCTCM3N3J3QW7B2EA  
Registration status: FORTICLIENT Disabled  
Compilation status: yes  
Configuration status: success  
Online status: online  
Offline grace status: Not allowed
```

[illegible]

In the example logs shown on this slide, **FortiTelemetry** is not enabled on FortiGate and, because of that, FortiClient is not able to find FortiGate. You can capture packets on the local PC to make sure packets are routed toward FortiGate, or run the sniffer on FortiGate to verify the traffic flow. Make sure to check the interface settings on the FortiGate.

You can run endpoint commands to verify the endpoint record and registration on FortiGate:

- Provides the IP address, registration status, online status, and so on, for the FortiClient endpoint

- Provides further details such as status, user, host OS, and serial number of the registration FortiGate

DO NOT REPRINT
© FORTINET

FortiClient and FortiGate

- Fortigate endpoint compliance diagnostic commands
 - `diagnose endpoint record-list <optional source IPv4>`
 - `diagnose endpoint record-summary`
 - `diagnose endpoint record-delete <optional source IPv4>`
 - `diagnose endpoint information`
 - `diagnose endpoint registration summary`
 - `diagnose endpoint registration list`
 - `diagnose endpoint registration block <FortiClient UID>`
 - `diagnose endpoint registration unblock <FortiClient UID>`
 - `diagnose endpoint registration deregister<all><FortiClient UID>`

FortiClient and FortiClient EMS

- Common issues
 - Unable to detect computers automatically
 - Unable to install, uninstall, or deploy changes
- Common causes
 - Computer browser services
 - Account permissions
 - Confirm required ports and Windows services are enabled
- Dashboard widgets
- Alerts and Logs messages

- Common alerts
 - New version of FortiClient is available
 - FortiClient deployment failed
 - Failure to check for signature updates
 - Error encountered when downloading AD server entries
 - Error encountered when scanning for local computers



There can be multiple dependencies and various factors involved when troubleshooting FortiClient and FortiClient EMS issues. Common issues can be that FortiClient is unable to detect automatically any computer running Microsoft Windows, you are unable to install or uninstall FortiClient from the host machine, or you are unable to deploy changes using FortiClient EMS.

You can resolve these issues by verifying the following:

Computer browser services: Automatically detects Microsoft Windows computers within the same local network. Make sure Computer Browser Services is running. For example, if the FortiClient EMS is installed on Windows 2012 R2 on which, by default, Computer Browser Service is disabled, FortiClient EMS will not detect computers on the same network, even if they are available.

Account permissions: Make sure the server and client have correct account permissions to deploy the changes. For example, if the administrator doesn't have the correct permissions to create or deploy the changes on FortiClient EMS or the client machine won't allow the account used for FortiClient EMS to make changes to the remote registry.

Confirm required ports and Windows services are enabled: FortiClient EMS uses many ports and services in order to communicate with clients and servers running associated applications. Make sure these ports and services, such as TCP 8013 used for FortiClient endpoint registration, Samba (SMB) service (port 445) and Distributed Computing Environment/Remote Procedure Calls (DCE- RPC) (port 135) used for FortiClient deployment, AD server connection 389, Windows (TCP port 80), Internet Information Services (IIS) (TCP port 443, 10443), and SQL server are enabled for use for FortiClient EMS. On the client side, make sure Task Scheduler is set to *Automatic*, Windows Installer is set to *Manual* and Remote Registry is set to *Automatic*.

FortiClient EMS has several dashboard widgets that provide information about managed clients and their current statuses. You can view alerts generated by FortiClient EMS by clicking the bell icon in the toolbar, which shows you alerts generated. An example of a common alert is "New version of FortiClient is available".

DO NOT REPRINT
© FORTINET

FortiClient and EMS Issues—View Logs

- Logs messages
 - Administrator > Logs
- Filter logs by date/time, level, source, and messages

10:56:35	Info	Update Service	Generated AV whitelist signature info (sig count=0, version=1.00000)
10:56:35	Debug	Update Service	Alert report generator will be next called at epoch 2147483647
10:56:35	Debug	Update Service	Checking/rebuilding EMS AV Whitelist
10:56:35	Debug	Update Service	ThreadRebuildSQLIndexes started
10:56:35	Info	Update Service	Service started
10:56:35	Debug	Update Service	Update daemon has started
16:36:36	Info	Repackager Service	Created 'FortiClient-6 (Windows)' installer.
16:36:32	Info	Console	BuiltInAdmin created Custom 6.0.3 Windows Installer: FortiClient-6.
11:41:26	Info	Console	BuiltInAdmin assigned Gateway List: Corporate FortiGate to forticlab.net.
11:39:23	Info	Console	BuiltInAdmin assigned Profile: Fortinet-Training to forticlab.net.
16:24:56	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 210 (Install started)
16:24:55	Info	Deployment Service	Started FortiClient installation task on forticlab.net\WIN-EHVKBEA3S71...
16:24:55	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 120 (Install task s...
16:24:55	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 80 (Installer copi...
16:24:51	Info	Deployment Service	Deploying FortiClient to forticlab.net\WIN-EHVKBEA3S71 forticlab.net
16:24:51	Info	Deployment Service	There are 10 licenses available and 1 devices pending installation. Ser...
16:24:50	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 70 (Pending depl...
16:24:50	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 50 (Probed)
16:24:47	Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 40 (Currently pro...

Engine/signature update

Console-profile and creation and assigning

Deployment service

FORTINET

12

You can view the logs on FortiClient EMS by clicking **Administrator > Logs**. You can filter logs by using various parameters and so on such as date/time, log level, source (such as **EMS Service**, **Update Service**, **AD Service**, and so on) and messages.

In the example shown on this slide, the logs provide detailed messages about the event occurred, which you can use to troubleshoot the issues with FortiClient and FortiClient EMS. You should change the log level to **Debug**.

On-net/Off-net Status

- Endpoint must connect FortiClient Telemetry to FortiGate and EMS
- Specifies on-net, off-net, or offline status
- FortiClient 6.0.1 with FortiGate and EMS 6.0.0 and later
 - Behind FortiGate and receives DHCP option 224 with serial number from FortiGate DHCP server
 - If no option 224, FortiClient specifies status based on EMS on-net/off-net settings
 - If no EMS settings, FortiClient specifies status based on on-net subnets from EMS
 - FortiClient sends the specified on-net/off-net status to EMS
- FortiClient 6.0.1 with FortiGate and EMS versions prior to 6.0.0
 - FortiGate specifies the on-net/off-net status
 - FortiClient sends the on-net/off-net status to EMS

FortiGate and EMS

The version of FortiOS and EMS affects how on-net, off-net, or online status is specified.

FortiClient 6.0.1 with FortiGate and EMS 6.0.0 and later

When FortiClient 6.0.1 with FortiGate and EMS 6.0.0 and later, FortiClient calculates on-net/off-net information. The following examples show how FortiClient specifies the endpoint status:

- The endpoint has an on-net status when the endpoint is behind a FortiGate and receives option 224 with the FortiGate serial number. In this case, FortiGate is the DHCP server, and FortiGate checks that the serial number matches its own serial number.
- If option 224 is not received or there is no match with the currently registered serial number, FortiClient specifies on-net/off-net status based on the DHCP on-net/off-net setting in EMS.
- If there is no EMS setting, FortiClient specifies on-net/off-net status based on the on-net subnets received from EMS
- FortiClient sends the specified on-net/off-net status to EMS

FortiClient 6.0.1 with FortiGate and EMS versions earlier than 6.0.0

- FortiGate specifies the on-net/off-net status
- FortiClient sends the on-net/off-net status to EMS

Note that you must remove `on-net` subnet setting from FortiClient XML manually before configuring `on-net` using EMS. When FortiGate and EMS are integrated, the primary FortiClient Telemetry connection is to FortiGate, and FortiGate calculates the status.

DO NOT REPRINT
© FORTINET

On-net/Off-net Status—FortiGate Only

- When there is no EMS server for management
 - On-net status when the endpoint is behind FortiGate and receives option 224
 - On-net status when the endpoint is inside one of the on-net subnets defined by FortiGate
 - Off-net status when the endpoint is outside of the FortiGate network
 - Offline status when the endpoint cannot connect Telemetry to FortiGate
 - Offline on-net status when the endpoint is inside the on-net network but can't connect Telemetry

FORTINET

14

FortiGate only

The versions of FortiClient and FortiOS do not affect the on-net, off-net, or online status. The following examples show how the endpoint status is specified when FortiClient is connected to FortiGate only:

- The endpoint has an on-net status when the endpoint is behind a FortiGate and receives option 224 with the FortiGate serial number. In this case, FortiGate is the DHCP server, and FortiGate checks that the serial number matches its own serial number.
- The endpoint has an on-net status when the endpoint is inside one of the on-net subnets defined by FortiGate. You can configure on-net subnets in the FortiClient Compliance profile using the FortiOS CLI and the set on-net addr command.
- The endpoint has an off-net status when the endpoint is outside of the FortiGate network, such as connected through an external interface or has not received option 224 with the FortiGate serial number.
- The endpoint has an offline status when the endpoint cannot connect FortiClient Telemetry to FortiGate and the endpoint is outside one of the on-net networks, even when option 224 and the FortiGate serial number are configured.
- The endpoint has an offline on-net status when the endpoint is inside one of the on-net networks, but cannot connect FortiClient Telemetry to FortiGate.

Note that for FortiClient to be in an on-net network, the IP address of FortiGate or EMS should be routed through the IP address from the on-net network.

DO NOT REPRINT
© FORTINET

On-net/Off-net Status—EMS Only

- FortiClient EMS only
- The following table shows how various configurations specify the endpoint status:

EMS DHCP on-net / off-net setting	On-net subnet	Option 224 serial number	Endpoint status
Off	No	N/A	On-net
On	No	Option not configured	Off-net
On	No	Option configured	On-net
Off or on	Yes and match	Configured or not	On-net
Off or on	Yes and do not match	Configured or not	Off-net

FortiClient EMS only

The FortiClient and EMS versions do not affect the on-net, off-net, or online status. The table on the slide shows how various configurations specify the endpoint status when FortiClient Telemetry is connected to EMS.

The following examples show how endpoint status is specified when FortiClient is connected to EMS only:

- The endpoint has an offline status when the endpoint cannot connect FortiClient Telemetry to EMS and is outside one of the on-net networks
- The endpoint has an offline on-net status when the endpoint cannot connect FortiClient Telemetry to EMS but is inside one of the on-net networks

Note that *On-net* subnets have higher priority over other settings. In addition, EMS does not compare the option 224 serial number. As long as the endpoint has the serial number, EMS assumes the endpoint is behind FortiGate and is on-net.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which method does FortiClient choose first for automatic registration?
 - A. Default gateway IP (FortiGate's IP)
 - ✓ B. Telemetry gateway IP list
2. Which device specifies on-net/off-net status in versions earlier than 6.0?
 - A. FortiClient EMS
 - ✓ B. FortiGate

DO NOT REPRINT
© FORTINET

Lesson Overview

- ✓ How to Approach FortiClient Issues
- ✓ Common Issues with FortiGate and EMS
- FortiClient Troubleshooting
- FortiClient EMS Troubleshooting
- FortiClient Features Troubleshooting

FORTINET

Good job! You now understand the diagnostics steps to resolve common issues between FortiClient and FortiClient EMS.

Now, you will learn about FortiClient components and troubleshooting.

FortiClient Troubleshooting

Objectives

- Understand FortiClient components on Windows:
 - FortiClient installation directory
 - FortiClient drivers
 - FortiClient registry keys
 - FortiClient Diagnostic Tool

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient components and troubleshooting, you will be able to resolve issues on Windows operating systems.

DO NOT REPRINT
© FORTINET

FortiClient TRBL—Installation Directory

- Default FortiClient installation directory
 - Windows 32 bit – C:\Program Files(x86)\Fortinet\FortiClient
 - Windows 64 bit – C:\Program Files\Fortinet\FortiClient
- Created during installation time
- Removed during uninstall
- Protected by FortiShield
- Does not contain drivers (sys) files
 - With the exception of mdare driver
- Contains .exe, .dll, logs, signatures, quarantined files
 - Creates folders for logs, quarantine, and signatures (vir_sig)

FORTINET

19

When FortiClient is installed on Windows OS, by default it is installed in `Program Files` on Windows 32-bit OS, and `Program Files (x86)` in Windows 64-bit OS. The FortiClient directory is created only during installation and removed during uninstallation.

You can change the default installation directory while installing FortiClient. FortiClient is protected by FortiShield, which is digitally signed and prevents modification of the Windows registry. The FortiClient folder contains .exe, .dll, logs, signatures, and quarantine files, and so on.

DO NOT REPRINT
© FORTINET

FortiClient TRBL—Installed FortiClient Files

- Some of the files installed in the FortiClient installation directory:

- forticlient.exe
- fortifw.exe
- fortitray.exe
- fortiesnac.exe
- fmon.exe
- submitv.exe
- fortiwf.exe
- vpcd.exe
- FortiSSLVPNdaemon.exe
- ipsec.exe
- mdare.dll
- libav.dll

FORTINET

20

When you install FortiClient, it installs a number of executables, dll, signatures, and so on, which includes:

- forticlient.exe – FortiClient GUI (FortiClient console)
- fortifw.exe – FortiClient personal firewall service
- fortitray.exe – FortiClient system tray controller
- fortiesnac.exe – Handles the endpoint control
- fmon.exe – FortiClient real-time file system monitor (FortiClient Realtime Anti-Virus Protection)
- submitv.exe – FortiClient virus submit daemon (FortiClient Virus Feedback Service)
- fortiwf.exe – FortiClient web filtering service
- vpcd.exe – FortiClient VPN policy retriever
- FortiSSLVPNdaemon.exe – FortiClient SSLVPN daemon
- ipsec.exe – FortiClient VPN Service
- mdare.dll – FortiClient malware detection and removal engine (malware detection and removal engine)
- libav.dll – Fortinet AV engine library (AV Engine Library)

DO NOT REPRINT
© FORTINET

FortiClient TRBL—FortiClient Drivers

- Default FortiClient driver location
 - Windows 32-bit – C:\Windows\SysWoW64\Drivers
 - Windows 64-bit – C:\Windows\System32\Drivers
- FortiClient drivers
 - fortifw2.sys
 - fortiwf2.sys
 - fortiloader.sys
 - FortiShield.sys
 - fortips.sys
 - fortisniff2.sys

FORTINET

21

When FortiClient is installed on Windows OS, it installs the necessary drivers on Windows 32-bit OS and Windows 64-bit OS, which includes:

- fortifw2.sys – FortiClient app firewall driver
- Fortiwf2.sys – FortiClient web filter driver
- fortiloader.sys – FortiClient fortiloader driver
- FortiShield.sys – FortiClient file system filter driver
- Fortips.sys – FortiClient IPsec driver
- fortisniff2.sys – FortiClient IPS driver

DO NOT REPRINT
© FORTINET

FortiClient TRBL—FortiClient Registry Keys

- HKLM\Software\Wow6432Node\Fortinet\FortiClient
 - Protected by FortiShield
- Cryptic
- Requires detailed knowledge
- Undocumented
- May or may not map to XML configuration
- No support on FortiClient GUI
- Intended for developers and corner cases

FORTINET

22

You can check the FortiClient registry keys at `HKLM\Software\Wow6432Node\Fortinet\FortiClient`. The registry keys are protected by **FortiShield**.

Unlike XML, registry keys are cryptic and the user requires detailed knowledge to configure. The keys can't be documented in any format and hence are not supported on the FortiClient GUI. The keys are intended for use by developers.

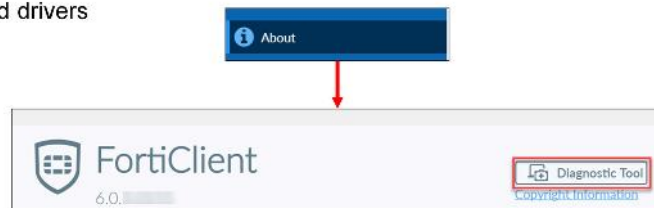
Note that in some cases Fortinet support can ask you to change the FortiClient registry or replace FortiClient files. To perform this task you must stop FortiShield first:

- Shutdown FortiClient
- In an elevated command-line window, type `sc stop fortishield`

DO NOT REPRINT
© FORTINET

FortiClient TRBL—Diagnostic Tool

- You can access the FortiClient Diagnostic Tool on the FortiClient console
 - Go to **About**
- FortiClient Diagnostic Tool generates a debug report
- FortiClient Diagnostic Tool does not record sensitive information
- It contains the following information about the endpoint:
 - Windows operating system version
 - Windows software updates
 - Names and versions of installed software
 - Names and versions of installed drivers
 - FortiClient configuration
 - FortiClient logs



FORTINET

23

You can use the FortiClient Diagnostic Tool to generate a debug report, and then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report, and send the report to customer support to help with troubleshooting.

The FortiClient Diagnostic Tool does not record sensitive information. It contains information about the endpoint, such as:

- Windows operating system version
- Windows software updates
- Names and versions of installed software
- Names and versions of installed drivers
- FortiClient configuration
- FortiClient logs

DO NOT REPRINT
© FORTINET

FortiClient TRBL—Logs

- You can export logs from FortiClient to review
- Change log level
- Default log level is **Information**



FORTINET

24

By default, the log level is set to **Information**, which provides enough related information to resolve common FortiClient issues. However, you can change the log level directly on FortiClient by clicking **Settings > Logging > Log Level** on a standalone FortiClient. In the case of a managed FortiClient (from FortiClient EMS), you can send the necessary configuration from **Endpoint Profile > System Settings** to FortiClient.

There are various log levels on FortiClient such as **Emergency, Alert, Information, Debug**, and so on. To get more detailed logs for debugging, change the log level to **Debug**.

Note that you can clear the check boxes next to feature(s) to reduce log entries when troubleshooting a specific feature issue.

DO NOT REPRINT
© FORTINET

FortiClient TRBL—BSOD

- Provide a kernel memory dump file
 - Located in: C:\windows\MEMORY.dmp
 - Enabling a kernel-mode dump File
 - <http://msdn.microsoft.com/en-us/library/windows/hardware/ff542953>
- If interested in reading the dump file, use WinDbg
 - Analysing a Kernel-Mode Dump File with WinDbg
 - <http://msdn.microsoft.com/en-us/library/windows/hardware/ff538042>
- To download WinDbg installer:
 - WDK and WinDbg downloads
 - <http://msdn.microsoft.com/en-us/windows/hardware/hh852365>
- Run and provide output of FortiClient_Diagnostic_Tool.exe
 - Collects system and FortiClient information for Fortinet support team
 - Useful when summarizing system

FORTINET

25

FortiClient can cause blue screen of death (BSOD) when it conflicts with third-party software. If this happens, provide a kernel memory dump. It is usually located in C:\windows\MEMORY.dmp

To configure the collection of dump files, refer to the following Microsoft documents:

- Enabling a kernel-mode dump file:

<http://msdn.microsoft.com/en-us/library/windows/hardware/ff542953>

- To reach the dump file, use WinDbg:

<http://msdn.microsoft.com/en-us/library/windows/hardware/ff538042>

- To download the WinDbg installer:

<http://msdn.microsoft.com/en-us/windows/hardware/hh852365>

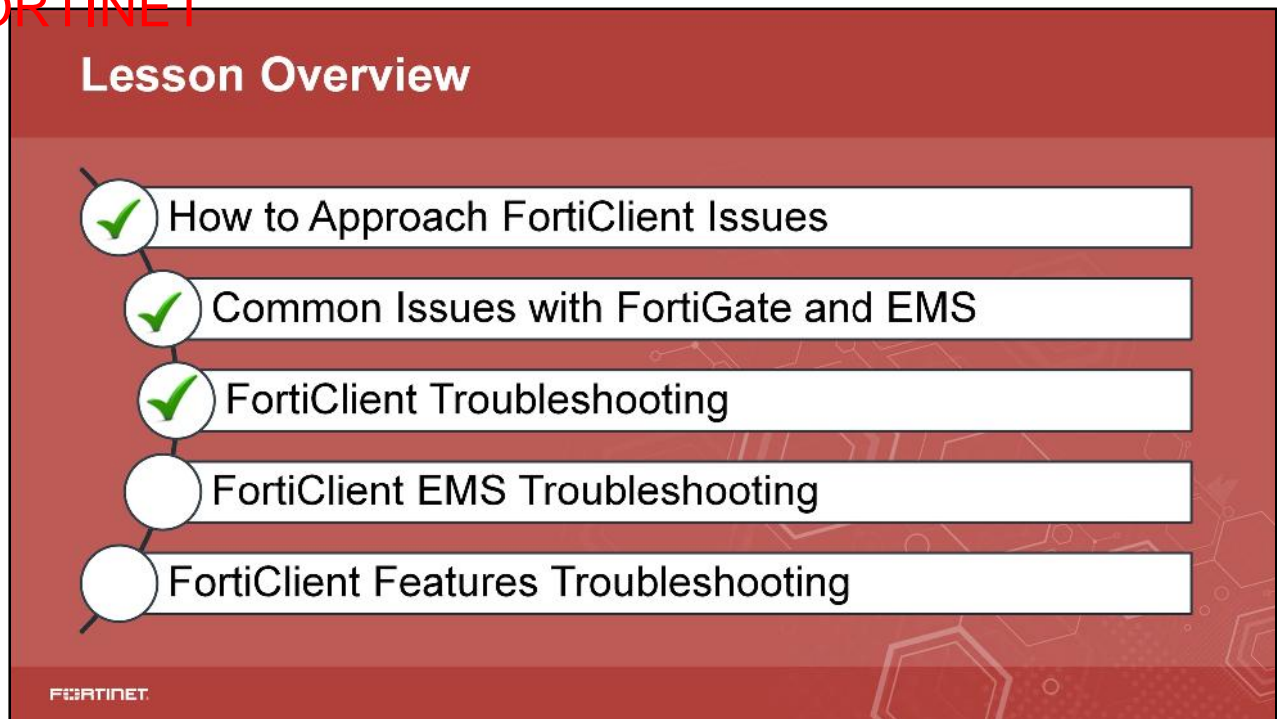
Run and provide the output of FortiClient_Diagnostic_Tool.exe.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. What protects FortiClient registry keys?
✓ A. FortiShield
B. FortiProxy
2. What is default log level in FortiClient?
A. Warning
✓ B. Information

DO NOT REPRINT
© FORTINET



Good job! You now understand FortiClient components and troubleshooting on Windows operating systems.

Now, you will learn about FortiClient EMS troubleshooting.

EMS Troubleshooting

Objectives

- Understand FortiClient EMS components on Windows:
 - FortiClient EMS installation directory
 - FortiClient EMS services
 - EMS Diagnostic Tool

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiClient EMS components and troubleshooting, you will be able to resolve EMS issues on Windows servers.

DO NOT REPRINT
© FORTINET

FortiClient EMS TRBL—Installation Directory

- Default FortiClient installation directory
 - Windows 64-bit – C:\Program Files (x86)\Fortinet\FortiClient
- Created during installation time
- Removed during uninstallation
- FortiClientEMS installs SQL Server 2014 Express Edition on the server
 - Doesn't remove the SQL Server during uninstallation
 - Instance=FCEMS
 - Service=mssql\$FCEMS
- FortiClientEMS also installs Apache HTTP Server and Python

FORTINET

29

By default, FortiClient EMS is installed in Windows `Program Files (x86)` on the Windows 64-bit OS. The FortiClient EMS directory is created only during installation and is removed during uninstallation.

You can change the default installation directory while installing FortiClient EMS. FortiClient EMS installs SQL Server 2014 Express edition on the server. FortiClient EMS doesn't remove SQL Server during uninstallation.

- Instance=FCEMS
- Service=mssql\$FCEMS

FortiClient EMS also installs Apache HTTP Server and Python.

DO NOT REPRINT
© FORTINET

FortiClient EMS TRBL—Installed Services

- List of services installed in FortiClient EMS installation directory:
 - FortiClient Enterprise Management Server
 - FcmDaemon.exe
 - FortiClient Enterprise Management Server Active Directory Service
 - FcmAdDaemon.exe
 - FortiClient Enterprise Management Server Apache Service
 - httpd.exe
 - FortiClient Enterprise Management Server for Chromebooks
 - FcmChromebookDaemon.exe
 - FortiClient Enterprise Management Server Update
 - FcmUpdateDaemon.exe
 - FortiClient Enterprise Management Server Deployment Service
 - FcmDeploy.exe
 - FortiClient Enterprise Management Server Monitor Service
 - FcmMonitor.exe

FORTINET

30

When you install FortiClient EMS, it installs a number of executables, dll, signatures, and so on, which includes:

- FcmDaemon.exe: For client connectivity/endpoint control/registration
- FcmAdDaemon.exe: For Active Directory groups
- httpd.exe: For EMS web console
- FA_Scheduler: Keeps track of all the EMS services and starts them when stopped
- FcmChromebookDaemon.exe: For Chromebooks management on FortiClient EMS
- FcmUpdateDaemon.exe: Connects to FortiGuard for updates
- FcmDeploy.exe: FortiClient deployment

DO NOT REPRINT
© FORTINET

FortiClient EMS TRBL—GUI Issue Debugging

- Using **Chrome > More tools > Developer tools > Network** to see the active connections from the EMS
 - C:\Program Files (x86)\Fortinet\FortiClientEMS\Apache24\logs
- More verbose logging:
 - /ProgramFiles/Fortinet/FortiClientEMS/Python/Scripts/FCM/FCM/Settings.py
 - Change *DEBUG* from "False" to "True"
- Apache uses port 443 and 10443

FORTINET

31

You can debug GUI access issues either by:

- Using a web browser
- Enabling verbose logging for Python

Make sure you turn off the debug after troubleshooting. You should not run the debug in a production environment. By default, apache uses port 443 and 10443. You can use `netstat` command to see if the default apache ports are being used by another application.

DO NOT REPRINT
© FORTINET

FortiClient EMS TRBL—View Debug Logs

- You can check logs on FortiClient EMS GUI
 - Administrator > Logs
- Change log level to **Debug**

Category	Time	Level	Source	Message	Frequency
Administration	15:30:42	Debug	Repackager Service	GetAssignedPackageInstallersPendingCreation() returned 0	2 times since 2019-02...
Administrators	15:30:42	Debug	Repackager Service	GetAssignedPackageInstallersPendingCreation() FortiClient-Version...	2 times since 2019-02...
User Server	15:30:42	Debug	Repackager Service	GetAssignedPackageInstallersPendingCreation() FortiClient-Version...	2 times since 2019-02...
User Settings	15:30:42	Debug	Repackager Service	GetAssignedPackageInstallersPendingCreation() FCTUInstaller (0...	1 time since 2019-02...
Group Assignment Rules	15:30:42	Debug	Repackager Service	GetAssignedPackageInstallersPendingCreation() FCTUInstaller (0...	2 times since 2019-02...
Backup Database	15:30:42	Debug	Repackager Service	GetAssignedPackageInstallersPendingCreation() FCTUInstaller (0...	1 time since 2019-02...
Restore Database	15:30:42	Debug	Repackager Service	"C:\Program Files (x86)\Fortinet\FortiClientEMS\Repackager.exe"	1 time since 2019-02...
Upgrade License	15:30:42	Debug	Repackager Service	Service started	2 times since 2019-02...
Logs	15:30:42	Debug	Repackager Service	SetAssignedEndPackageInstallers() returned 0	2 times since 2019-02...
System Settings	15:30:42	Debug	Repackager Service	SetAssignedEndPackageInstallers() vson=not id=3, installation...	1 time since 2019-02...
	15:30:42	Debug	Repackager Service	EndUpdateResource() returned 1 (err=0)	2 times since 2019-02...
	15:30:42	Debug	Repackager Service	UpdateResource() returned 0 (err=0)	2 times since 2019-02...

- However this doesn't include FortiClient EMS installation logs
- For FortiClient EMS installation issues go to:
 - C:\Users\Administrator\AppData\Local\Temp\FortiClient_Enterprise
- SQL Server installation logs
 - %temp%\sql

FORTINET

32

On FortiClient EMS, you can see the logs on **Administrator > Logs**. To get more information, you should to change the log level to **Debug**. However this GUI log doesn't include FortiClient EMS and SQL installation logs. Installation logs are generally available in the temp folder.

Note that FortiClient EMS automatically reverts the log level from **Debug** to **Info** after 30 minutes to save resources on server. EMS GUI only displays logs from database, daemon debug logs are sent to the file only.

DO NOT REPRINT
© FORTINET

FortiClient EMS TRBL—Diagnostic Tool

- You can access the FortiClient Diagnostic Tool in:
 - C:\ProgramFile(x86)\Fortinet\FortiClientEMS
- FortiClientEMS Diagnostic Tool generate a debug report
- FortiClient Diagnostic Tool does not record sensitive information
- It contains the following information about the endpoint:
 - Windows operating system version
 - Server event logs
 - FortiClientEMS Apache configuration
 - FortiClientEMS Apache logs
 - FortiClientEMS logs
 - Names and versions of installed software
 - Names and versions of installed drivers
 - Python logs
 - Temp directory installation logs



FORTINET

33

You can use the FortiClient EMS Diagnostic Tool to generate a debug report, and then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report, and send the report to customer support to help with troubleshooting.

The FortiClientEMS Diagnostic Tool does not record sensitive information. It contains information about the endpoint, such as:

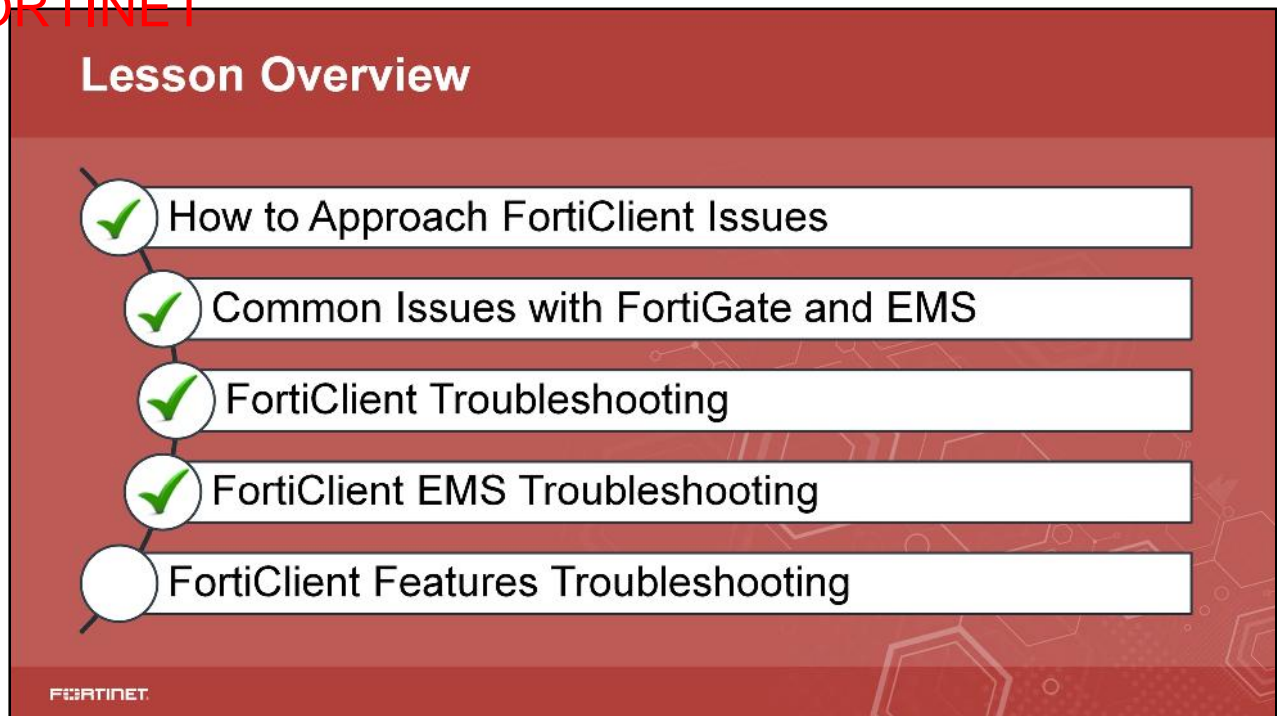
- Windows operating system version
- Server event logs
- FortiClient EMS Apache configuration
- FortiClient EMS Apache logs
- FortiClient EMS logs
- Names and versions of installed software
- Names and versions of installed drivers
- Python logs
- Temp directory installation logs

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which database is installed with the EMS installation?
 - A. Oracle
 - ✓ B. Microsoft SQL Server
2. Which process is responsible for the EMS web console?
 - A. FcmDaemon.exe
 - ✓ B. httpd.exe

DO NOT REPRINT
© FORTINET



Good job! You now understand FortiClient EMS components and troubleshooting on Windows Servers systems.

Now, you will learn about diagnosing and troubleshooting FortiClient features.

DIAGS and TRBL: FortiClient Features

Objectives

- Diagnose FortiClient features:
 - Update
 - Antivirus (real-time protection)
 - Sandbox
 - Web filter
 - VPNs—SSL and IPsec
 - Application control
 - Vulnerability scan
 - Telemetry and compliance

FORTINET

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in diagnosing FortiClient features, you will be able to resolve issues related to individual features.

FortiClient Features—Updates

- Verify on FortiClient console for latest updates
 - On left pane, click **About**
 - Run manually in an elevated command line window
 - `update_task.exe -s fd_01`
- Registry
 - FA_UPDATE
 - FA_Scheduler\00003
- Check XML configuration
 - `<forticlient_configuration> <system> <update>`
 - Check custom servers if defined
 - Backup server
 - Failover to FDN
 - Schedule update

Engines		
Name	Status	Version
AntiVirus	Up To Date	6.0002
Anti Rootkit	Up To Date	2.0002
Signature	Up To Date	2.0002

Signatures		
Name	Status	Version
AntiVirus	Up To Date	6.0002
AntiRootkit	Up To Date	2.0002
AntiVirus Engine	Up To Date	6.0002
Signature	Up To Date	2.0002
IPS Signatures	Up To Date	6.0002

```
<update>
  <use_custom_server>0</use_custom_server>
  <restrict_services_to_regions>
  <server>
    <port>888</port>
    <timeout>60</timeout>
    <failoverport>
    <fail_over_to_fdn>0</fail_over_to_fdn>
    <use_proxy_when_fail_over_to_fdn>0</use_proxy_when_fail_over_to_fdn>
    <auto_patch>0</auto_patch>
    <submit_virus_info_to_fds>0</submit_virus_info_to_fds>
    <submit_vuln_info_to_fds>0</submit_vuln_info_to_fds>
    <update_action>notify_only</update_action>
    <scheduled_updates>
      <enabled>0</enabled>
      <type>Interval</type>
      <daily_at>01:00</daily_at>
      <update_interval_in_hours>1</update_interval_in_hours>
    </scheduled_updates>
  </update>
```

FORTINET

37

The FortiClient console provides the latest information regarding engine and software statuses and versions used by FortiClient. To check the latest updates on FortiClient, click **About**.

By default, the value for `<use_custom_server>` is 0, which means it is disabled, failover backup servers are not defined, and failover to public FDN is enabled. In this case, FortiClient will first attempt to connect to the public FortiClient server `forticlient.fortinet.net` or `myforticlient.fortinet.net` over TCP port 80 to download the list of secondary servers from which it will then download the signatures and packages for FortiClient.

If a string is specified in `<server>` and communication fails with that server, each of the servers specified in `<fail_over_servers>` are tried until one succeeds. If that also fails, then software updates will not be possible unless `<fail_over_to_fdn>` is set to 1. If communication fails with the server(s) specified in both `<server>` and, `<fail_over_servers>`, `<fail_over_to_fdn>` specifies the next course of action.

You should leave the default value of `<fail_over_to_fdn>` set to 1.

By default, scheduled updates are enabled at an intervals, this specifies the frequency that FortiClient checks for updates. A network error will cause an update failure, and the temporary AV signatures keep growing. Run the `update_task` command manually.

DO NOT REPRINT
© FORTINET

FortiClient Features—Updates

- Signature update logs
 - **Settings > Export Logs**
 - Can be opened with any text editor

```

6:33:25 AM    Notice    Update    id=96650
avsig=28.00220 avsigetm=28.00105 avsigext=28.00083
avsigheu=28.00220 avsiglastupdate="06:33:11-06"
ipssig=6.00699 irdbsig=2.00502

```

- Software update logs
 - Located in %temp% folder in Windows
 - C:\Users\<username>\AppData\Local\Temp\

FORTINET

30

The signature update logs provide the date and time of the update along with the version number of the signatures. To export the logs to a local computer from FortiClient, click **Settings > Export Logs**. Based on the logging level and log types enabled it will export all types of logs.

The software update logs are located in the %temp% folder in Windows, which might be a hidden folder.

FortiClient Features—AntiVirus

- Files and drivers – .exe, .dll, .sys, .conf
 - fmon.exe, xmlav.dll, libav.dll, mdare.dll, mdare.sys
- vir_sig folder contains
 - Malware and Antivirus signatures
 - Mdare_sig, vir_ext, vir_extreme, vir_heuristics, vir_high, vir_high
 - fdni.conf—list of FortiGuard servers
 - Block malicious websites
 - fortiwf.exe, fortiwf2.sys
 - Block known communication channels
 - fortifws.exe, fortisniff.sys, irdb.dat

```

SerialNumber=FPT-FCS-29500013|Address=208.91.112.135:443|FDNListener=208.91.112.135:8889|TimeZone=-5
SerialNumber=FPT-FCS-DELL0005|Address=208.91.112.132:443|FDNListener=208.91.112.132:8889|TimeZone=-5
SerialNumber=FPT-FCS-DELL0008|Address=208.91.112.133:443|FDNListener=208.91.112.133:8889|TimeZone=-5
SerialNumber=FPT-FCS-DELL0015|Address=208.91.112.136:443|FDNListener=208.91.112.136:8889|TimeZone=8

```

FortiClient requires a number of files and drivers in order to perform a real-time antivirus scan which includes exe, dll, sys, and conf files, and are located in Installation directory\Fortinet\FortiClient\ folder. The vir_sig folder contains malware and antivirus signatures along with the fdni.conf file which contains a list of public FortiGuard servers that FortiClient contacts to get updates on the signatures and packages.

DO NOT REPRINT
© FORTINET

AntiVirus—Real-Time Protection

- Check XML configuration
 - `<forticlient_configuration> <antivirus> <real_time_protection>`
- Fmon

```
<real_time_protection>
<enabled>1</enabled>
<use_extreme_db>0</use_extreme_db>
<when>0</when>
<ignore_system_when>2</ignore_system_when>
<on_virus_found>5</on_virus_found>
<cloud_based_detection>
  <on_virus_found>4</on_virus_found>
</cloud_based_detection>
<compressed_files>
  <scan>1</scan>
  <maxsize>10</maxsize>
</compressed_files>
```

Compressed file size to scan in MB

```
<scan_file_types>
<all_files>1</all_files>
<file_types>
  <extensions>.JPG,.ACE,.ACM,.ADV,.ACK,.ADT,.APP,.ASD,.ASP,.ASN,.AVB,.AX,.A
  Xs,.BAI,.BIN,.BIN,.CDR,.CFM,.CHM,.CLA,.CLASS,.CMD,.CMM,.COM,.CPL,.CPT
  ,.CPY,.CSC,.CSH,.CSS,.DEV,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FO
  N,.GMS,.GVB,.HLP,.HTA,.HTM,.HTML,.HTI,.HTW,.HTX,.HXS,.INF,.INI,.JPG,.
  JS,.JTD,.RSE,.LOG,.LIS,.LNX,.MBS,.MHT,.MHTM,.MOD,.MPD,.MPF,.MP
  T,.MOC,.OCX,.PDF,.PL,.PSG,.PM,.RHF,.RUP,.POT,.PPS,.PPT,.PPC,.PPT
  ,.QIB,.QPW,.REG,.RTF,.SBF,.SCR,.SCT,.SH,.SRB,.SRS,.SRT,.SHIML,.SRM,.S
  IS,.SMX,.SNF,.SYS,.TDO,.TLB,.TSK,.TSF,.TTF,.VBA,.VBE,.VBS,.VEN,.VOM,.
  VSD,.VSS,.VST,.VWF,.VXD,.VXE,.WBK,.WBT,.WIZ,.WM,.WMG,.WPC,.WPD,.WSC,.
  WST,.WSH,.XLS,.XML,.XTP</extensions>
  <include_files_with_no_extensions>1</include_files_with_no_extensions>
</file_types>
</scan_file_types>
```

FORTINET

40

It is very important to check the XML configuration if the real-time antivirus protection is not functioning properly. By default, when a virus is found, FortiClient quarantines the file. There are five levels of `<on_virus_found>` XML configuration tags:

- 0: clean
- 1: ignore
- 2: repair
- 3: warning
- 4: quarantine
- 5: deny access

FortiClient also performs a scan on the compressed files and allows you to define the compressed file size to scan up to 65535MB. 0 means no limit. FortiClient performs a real-time scan on a wide range of extensions and allows you to modify the list of extensions to scan.

For example, if you set the value of the `<on_virus_found>` XML configuration tag to 1, it will ignore the virus file and the virus will not be caught. Another example is if you modify and remove a few extensions from the `<extensions>` XML configuration element and if the suspicious file extension is not listed in the `<extensions>` XML configuration element, it will be not caught.

Note that this partial XML configuration is for a real-time antivirus. For a complete list of available XML configuration elements, refer to the *FortiClient 6.0.0 XML Reference guide* available at <http://docs.fortinet.com>.

AntiVirus—Real-Time Protection (Contd)

- FortiClient Logs

- Settings > Logging > Export logs
- Installation directory\Fortinet\FortiClient\logs\realtime_scan.log

Exported logs

15 9:44:37 AM	Notice AntiVirus	id=96533 user=	msg="User enabled Realtime AntiVirus protection"
15 9:44:49 AM	Warning AntiVirus	id=96530 user=	action=quarantined checksum=0x31db20d1 filesize=184
msg="Found virus by AntiVirus realtime protection, in filesystem" sigid=439872 virus=EICAR_TEST_FILE			
File=C:\Users\ \AppData\Local\Temp\UI07JCnC.zip.part			

realtime_scan.log

realtime_scan - Notepad			
File	Edit	Format	View Help
Realtime scan result:			
time: 09:44:39	Realtime Protection Started,	AV_ENGINE:5.00220 MDARE_ENGINE:2.00060	AV_SIG:28.00336 AV_EXT_SIG:28.00226 MDARE_SIG:1.00000
time: 09:44:48	virus found: EICAR_TEST_FILE	action: Quarantined, C:\Users\ \AppData\Local\Temp\UI07JCnC.zip.part	

The antivirus logs provides the date and time of the real-time antivirus scan along with the action taken, virus, and location of the file. To export the logs to a local computer from FortiClient, click **Settings > Logging > Export Logs**.

Based on the logging level and log types enabled, **Export Logs** will export all types of logs.

The realtime_scan.log located in Installation directory\Fortinet\FortiClient\logs\realtime_scan.log provides more detailed information regarding malware and antivirus engines and signatures used in the real-time antivirus scan along with name of the virus file, action taken, and location of the file.

Debug: Command line - In an elevated command line window:

- Disable RTP from the GUI OR shut down FortiClient
- Change directory into FortiClient installation directory `fmon.exe -s -fd_1`

AntiVirus—Real-Time Protection (Contd)

- RTP for other security risks protection
 - Sandbox
 - `<use_sandbox_signatures>0</use_sandbox_signatures>`
 - Block malicious websites
 - `<forticlient_configuration><webfilter><block_malicious_websites>`
 - Block known attack communication channels
 - `<forticlient_configuration><firewall><candc_enabled>`
 - Email protection
 - `<forticlient_configuration><antivirus><email>`

```
<email>
  <smtp>1</smtp>
  <pop3>1</pop3>
  <outlook>1</outlook>
  <wormdetection>
    <enabled>0</enabled>
    <action>0</action>
  </wormdetection>
  <heuristic_scanning>
    <enabled>0</enabled>
    <action>0</action>
  </heuristic_scanning>
  <mime_scanning>
    <enabled>0</enabled>
  </mime_scanning>
</email>
```

There are other security risks that are handled by real-time protection:

Sandbox signatures:

- FortiClient uses sandbox signatures to identify the threat.

Block malicious website:

- Block access to malicious websites. The web filter module must be installed before you can enable this protection.

Block known attack communication channels:

- Select to block known communication channels used by attackers. The application firewall module must be installed before you can enable this protection.

Email protection:

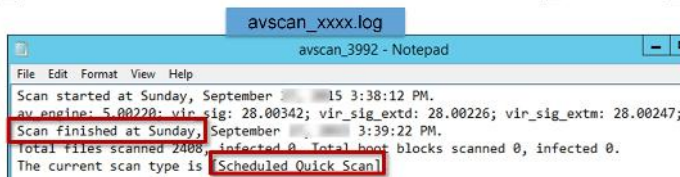
- Scans email for malicious files. Support POP3 and SMTP.

You can use Boolean values to enable or disable real-time protection features. For example,

`<block_malicious_websites>0</block_malicious_websites>` will disable blocking of malicious websites.

AntiVirus—Schedule and Custom Scan

- Uses same files and drivers as real-time antivirus scan
 - Uses `av_task.exe` instead of `fmon.exe`
 - `av_task.exe <options>`
 - `-q` - quick scan
 - `-f` - full system scan
 - `-d <dir>` - scan the specified directory
 - `-x` - use multiple `av_task.exe` instances for scanning
- Check XML configuration
- `<forticlient_configuration> <antivirus> <scheduled_scan>`
- `<forticlient_configuration> <antivirus> <on_demand_scanning>`
- FortiClient Logs



FORTINET

43

The scheduled and custom scan uses the same real-time antivirus files and drivers except it uses `av_task.exe` instead of `fmon.exe`.

- `av_task.exe -f`
- `av_task.exe -d c:\users`

The factory default at the time of installation is to run a full system scan on the first day of the month at 18:30 hours and it also scans removable media. The following is part of the partial default XML configuration for a full system scan which can be modified.

```
<full>
<enabled>1</enabled>
<repeat>1</repeat>
<day_of_month>1</day_of_month>
<time>18:30</time>
<removable_media>1</removable_media>
<network_drives>0</network_drives>
<priority>0</priority>
</full>
```

By default, the priority of the scan is set to normal and has three different levels:

- 0: normal
- 1: low
- 2: high

The `<on_demand_scanning>` element defines how the antivirus scanner handles the scanning of files manually requested by the end user. The scheduled and on-demand scan logs are located in `InstallationDirectory\Fortinet\FortiClient\logs\av_scanxxxx.log`

DO NOT REPRINT
© FORTINET

FortiClient Features—Sandbox Detection

- Files and drivers
 - `fortiAptFilter.sys`
 - `fcaptmon.exe`
 - `vir_sandbox_sig`
- Registry
 - `FA_SANDBOX`
 - `FA_Scheduler/000022`
- XML
 - `<forticlient_configuration><sandboxing>`
- Maximum file size is 200MB
- Command-line: `Fcaptmon.exe -s fd_01`
- FortiSandbox cache improves performance for same downloaded files
 - `Fcaptmon.apr`: cache file used by `fcaptmon.exe`
 - `Aptcache.dat`: cache file used by sandbox driver

FORTINET

44

The FortiClient requires a number of files and drivers in order to perform file submission to FortiSandbox. The `vir_sanbox_sig` folder contains malware and antivirus software. The maximum file size you can submit from FortiClient to FortiSandBox is 200MB.

Files can be submitted from the following sources:

- Removable media
- Mapped network drives
- Web downloads
- Email download

You can run a sandbox debug by entering the CLI command `Fcaptmon.exe -s fd_01` in an elevated command-line window.

FortiSandbox also caches files to improve performance.

FortiClient Features—Web Filter/Security

- Files and drivers
 - fortiproxy.exe, fortiWF.exe, xmlwf.dll, fortiWF.sys
- Check XML configuration
 - <forticlient_configuration> <webfilter>

```
<webfilter>
<enable_filter>1</enable_filter>
<enabled>1</enabled>
<current_profile>0</current_profile>
<max_violations>5000</max_violations>
<max_violation_age>7</max_violation_age>
<block_malicious_websites>1</block_malicious_websites>
<browser_read_time_threshold>180</browser_read_time_threshold>
```

Web filtering enabled
by default

FortiGuard querying
service

- FortiClient logs
 - View recent violations on FortiClient GUI
 - Settings > Logging > Export logs**

Web Filter Enabled [Disable](#)

Web Filter helps protect you by filtering web access based on more than 75 web content categories and more than 43 million rated websites - all continuously updated via FortiGuard Labs.

Sites Blocked (in last 7 days): [1](#)

Violations

[Clear Violations](#)

URL	CATEGORY	TIME	USER
www.sportsmanguncentre.co.uk	Weapons (Sales)	14:21:09	

FORTINET

45

FortiClient requires a number of files and drivers in order to perform web filtering. By default, web filtering and the FortiGuard querying service is enabled and can store up to 5000 violations for a period of seven days. The default value for <max_violations> is set to 5000 and can be ranged from 250 to 5000, and <max_violation_age> is set to seven days and can be ranged from 1 to 90 days.

You can also configure safe search and the YouTube education filter under the <safe_search> and <youtube_education_filter> XML elements.

For complete list of available XML configuration elements, refer to the *FortiClient 6.0.0 XML Reference guide* available at <http://docs.fortinet.com>

Safe Search: Safe Search is a feature of Google search that acts as an automated filter of pornography and potentially offensive content. In the upcoming release of FortiClient we will have the ability to modify the host file to force all Google or Youtube traffic to connect to safe search websites such as **WackySafe** that only delivers safe search results. Drawback is that this will affect all Google services, such as search, Youtube, and so on.

You can view the web filtering violation logs directly on the FortiClient GUI or export the logs by clicking **Settings > Logging > Export logs**.

FortiClient Features—Web Filter/Security (Contd)

• FortiClient logs

```

2007/06/05 4:16:56 PM Notice WebFilter date=2007/06/05 time=16:16:55
logver=2 type=traffic level=info sessionid=34973356 hostname=NTN-81BESU9FULP
uid=89054F3525124328A62F432C52F5562E devid=FC78003460228176
[redacted] regip=N/A srcname=firefox.exe srcproduct=firefox
srcip=10.0.1.10 srcport=54346 direction=outbound destinationip=66.171.121.44
remotenname=www.fortinet.com destinationport=80 user=Saurabh proto=6 rcvbyte=N/A
sentbyte=N/A utmaction=passthrough utmevent=webfilter threat="General Interest -
Business:Information technology vdrroot=vtver=25.0 os="Microsoft
Windows Server 2012 R2 Datacenter Edition, 64-bit (build 9600)"
usingpolicy="Training" service=http url=index.html userinitiated=0
browsetime=N/A

2007/06/05 4:40:12 PM Notice WebFilter date=2007/06/05 time=16:40:12
logver=2 type=traffic level=warning sessionid=34973356 hostname=NTN-81BESU9FULP
uid=89054F3525124328A62F432C52F5562E devid=FC78003460228176 [redacted]
regip=N/A srcname=firefox.exe srcproduct=firefox srcip=10.0.1.10 srcport=55672
direction=outbound destinationip=23.235.39.81 remotename=www.bbc.com
destinationport=80 user=Saurabh proto=6 rcvbyte=N/A sentbyte=N/A
utmaction=blocked utmevent=webfilter threat="General Interest - Personal:News
and Media vdr=N/A vtver=N/A os="Microsoft Windows Server 2012 R2
Datacenter Edition, 64-bit (build 9600)" usingpolicy="" service=http url=/
userinitiated=1 browsetime=N/A

```

• Webfilter cache file

- urlcache.dat

• Debug CLI commands

- `fortiwf.exe -s fd_01`
- `fortiproxy.exe -s fd_01 -d 4`

FORTINET

45

In the example shown on this slide, the first log entry is from a FortiClient that is managed by EMS and FortiGate (integrated mode). The managed FortiClient log will show the FortiGate serial number along with the name of the FortiClient profile it is using, and other details such as utmaction, utmevent, and so on.

The second log entry is from the standalone FortiClient, which doesn't have the information regarding the FortiGate serial number and policy.

So, when diagnosing and troubleshooting web filtering issues, always pay attention to the logs because the URL or category might be blocked in the managed profile, and not in the standalone profile, and the results might be different than what you were expecting.

The webfilter cache URL rating results in the `urlcache.dat` file. You can also run the following CLI commands in elevated mode to further troubleshoot webfilter issues:

- `fortiwf.exe -s fd_01`
- `fortiproxy.exe -s fd_01 -d 4`

DO NOT REPRINT
© FORTINET

FortiClient Features—IPSec VPN

- Files and drivers
 - ipsec.exe (IPSec daemon)
 - FCAuth.exe (involved in IPSec certificate)
 - Fortips.sys
 - FortiFilter.sys
 - ftnic.sys
- Registry
 - FA_IKE
 - IPSec
 - FA_VPN
 - FA_Scheduler\000002
- XML
 - `<forticlient_configuration><vpn><ipsecvpn>`

FORTINET

47

FortiClient requires a number of files and drivers for IPSec VPN.

The VPN-related information is contained inside the `<VPN>` `</VPN>` XML tags. The `<options>` XML tag contains global options that apply to both SSL VPN and IPsec VPN:

```
<forticlient_configuration><vpn><options>
```

The `<ipsecvpn>` XML tag contains configurations specifically related to IPsec VPN.

IPsec VPN has two subsections:

- Options: Options related to the specific type of VPN.
- Connections: User defined connections.

FortiClient Features—IPSec VPN (Contd)

- FortiClient logs
 - File Settings > Logging > Export logs
 - Change log level to Debug
 - Optionally disable other types of logging

```

2:51:25 PM Debug VPN ===
2:51:25 PM Debug VPN initiate new phase 1 negotiation: 172.26.33.156[500]<=>10.0.0.1[500]
2:51:25 PM Debug VPN begin Aggressive mode.
2:51:25 PM Debug VPN new cookie: e710f7549f544d54
2:51:25 PM Debug VPN use ID type of IPv4_address
2:51:25 PM Debug VPN compute DH's private.
2:51:25 PM Debug VPN 7466cad5 77673ec1 717f3443 c2509c48 f62f7209 95eef934 826ba073 1bf914fa
2:51:25 PM Debug VPN compute DH's public.
2:51:25 PM Debug VPN 81614101 8218c29b 5abbec68 138dd412 3d5abb34 23d69c9b b3117092 45575831
2:51:25 PM Debug VPN authmethod is psk-shared key
2:51:25 PM Debug VPN add payload of len 96, next type 4
2:51:25 PM Debug VPN add payload of len 192, next type 10
2:51:25 PM Debug VPN add payload of len 16, next type 5
2:51:25 PM Debug VPN add payload of len 8, next type 13
2:51:25 PM Debug VPN add payload of len 16, next type 13
2:51:25 PM Debug VPN (repeated 3 times in last 0 sec) add payload of len 16, next type 13
2:51:25 PM Debug VPN add payload of len 8, next type 13
2:51:25 PM Debug VPN add payload of len 16, next type 13
2:51:25 PM Debug VPN (repeated 1 times in last 0 sec) add payload of len 16, next type 13
2:51:25 PM Debug VPN add payload of len 16, next type 0
2:51:25 PM Debug VPN 508 bytes from 172.26.33.156[500] to 10.0.0.1[500]
2:51:25 PM Debug VPN sockname 0.0.0.0[500]
2:51:25 PM Debug VPN send packet from 172.26.33.156[500]
2:51:25 PM Debug VPN send packet to 10.0.0.1[500]
2:51:25 PM Debug VPN 1 times of 508 bytes message will be sent to 10.0.0.1[500]
2:51:25 PM Debug VPN e710f754 9f544d54 00000000 00000000 01100400 00000000 000001fc 04000064
2:51:25 PM Debug VPN resend phase1 packet e710f7549f544d54:0000000000000000
2:51:25 PM Information VPN id=96566 msg="negotiation information, loc_ip=172.26.33.156 loc_por
2:51:27 PM Debug VPN CHKPHITHERE: no established phi handler found
2:51:27 PM Debug VPN (repeated 1 times in last 1 sec) CHKPHITHERE: no established phi handle

```

FORTINET

48

VPN-related logs can be exported from **Settings > Logging > Export logs**. When troubleshooting VPN issues, as a best practice, change the log level to **Debug** and disable other types of logging to minimize the logs from other features.

The FortiClient-FortiGate dialup request is sent from FortiClient towards FortiGate. The FortiClient-FortiGate negotiates using aggressive mode. In aggressive mode, the IKE SA contains almost everything, such as the encryption type, length, hash type, and Diffie-Hellman (DH) group. It contains fewer exchanges and packets and is faster than main mode.

DO NOT REPRINT
© FORTINET

FortiClient Features—IPSec VPN Debug

- Debug
 - Change log level on FortiClient
 - Enable IKE debug on FortiGate
 - `diag debug application ike -l`
 - `diag debug application fndamd -l`
 - `diag debug enable -l`
- Capture network traffic on both FortiClient host and FortiGate
- You can also initiate IPSec from the CLI
 - `Ipsec.exe [-d debuglevel] [-i sessionid] [-b] [-k] tunnel`
 - `ipsec.exe -U fortinet -P st70ngP@ssw07d prague_off`

FORTINET

49

You can run the real-time debug commands on FortiGate, which will show you the similar information as on FortiClient.

As a best practice, run the debug commands on FortiGate to compare with the IPSec VPN logs on the FortiClient.

Apart from the real-time debug command shown on the slide, you can also run the following commands to troubleshoot IPSec VPN issues:

- Check the configuration as it is seen by IKE daemon: `diagnose vpn ike config list`
- List IKE SA: `diagnose vpn ike gateway list`
- List IPsec SA: `diagnose vpn tunnel list`
- Check status of all tunnels (equivalent to GUI VPN monitor): `get ipsec tunnel list`
- Check routes that were installed by the IKE daemon (applicable only for dialup IPSec VPN): `diagnose vpn ike routes list`

DO NOT REPRINT
© FORTINET

FortiClient Features—SSL VPN

- Files and drivers
 - FortiSSLVPNdaemon.exe
 - ftsvnic.sys (new driver)
 - pppop.sys (old driver)
- Registry
 - FA_SSLVPN
 - Sslvpn
 - FA_VPN
 - FA_Scheduler\000019
- XML
 - <forticlient_configuration><vpn><sslvpn>

The FortiClient requires a number of files and drivers for SSL VPN.

The <sslvpn> XML tag contains configurations specifically related to SSL VPN.

SSL VPN has two subsections:

- Options: Options related to the specific type of VPN.
- Connections: User defined connections.

FortiClient Features—SSL VPN (Contd)

- FortiClient Logs
 - **File Settings > Logging > Export logs**
 - Change log level to **Debug**
 - Optionally disable other types of logging

SSL VPN initiated

```

3:53:03 PM Debug VPN (repeated 142 times in last 324 sec) FortiSslvpn: CSslvpnBase::RefreshConnection() Called.
3:53:05 PM Debug VPN FortiSslvpn: proxy flag: 1 proxy:(null)
3:53:05 PM Debug VPN FortiSslvpn: CSslvpnBase::OnConnect(): Before check server TCP port. *****
3:53:05 PM Debug VPN FortiSslvpn: CSslvpnBase::InitFortiSslvpn() Called.
3:53:05 PM Debug VPN FortiSslvpn: CSslvpnBase::InitFortiSslvpn(): Daemon is running
3:53:05 PM Debug VPN FortiSslvpn: SslvpnAgent: before connect pipe
3:53:05 PM Debug VPN FortiSslvpn: SslvpnAgent: before create file
3:53:05 PM Debug VPN FortiSslvpn: SslvpnAgent: ActiveX connected to SslvpnDaemon
3:53:05 PM Debug VPN FortiSslvpn: CSslvpnBase::InitFortiSslvpn(): SslvpnAgent initialized successfully
3:53:05 PM Debug VPN FortiSslvpn: >>>>DoConnect(fr.fortinet.com:443) ...
3:53:05 PM Debug VPN FortiSslvpn: GetWebPage(): URL=/remote/info -->
3:53:05 PM Debug VPN FortiSslvpn: =====
3:53:05 PM Debug VPN FortiSslvpn: <?xml version='1.0' encoding='utf-8'?><info><api snameshod='0' salt='51479555' remotesshtimeout='30' f='f' /></info>
3:53:05 PM Debug VPN FortiSslvpn: =====
3:53:05 PM Debug VPN FortiSslvpn: GetWebPage(): bRC=1,CT=(text/xml; charset=utf-8)

```

VPN connected

```

3:53:27 PM Information VPN FortiSslvpn: 7624: fortissl_connect: device=Clynic
3:53:27 PM Information VPN FortiSslvpn: 13908: PreferDTLS Tunnel=0
3:53:28 PM Debug VPN FortiSslvpn: <<<<DoConnect(): bRC=1, ErrorCode=0
3:53:28 PM Debug VPN FortiSslvpn: CSslvpnBase::OnConnect(): DoConnect()==TRUE *****
3:53:28 PM Debug VPN FortiSslvpn: CSslvpnBase::OnConnect(): SSL VPN Tunnel is Connected *****
3:53:28 PM Debug VPN FortiSslvpn: CSslvpnBase::RefreshConnection() Called.
3:53:31 PM Debug VPN (repeated 2 times in last 4 sec) FortiSslvpn: CSslvpnBase::RefreshConnection() Called.
3:53:34 PM Notice VPN date=2019-02-26 time=15:53:33 logver=1 type=traffic level=notice sessionId=165643392 hostname= podomain
3:53:34 PM Information VPN id=96600 user=" " msg="SSLVPN tunnel status" vpnstate=connected vpnkunnel="SSL - " vntype=ssl

```

FORTINET

51

You can export VPN-related logs by clicking **Settings > Logging > Export logs**. When troubleshooting VPN issues, as a best practice change the log level to **Debug** and disable other types of logging to minimize the logs from other features.

The FortiClient-FortiGate SSLVPN request is sent from FortiClient towards FortiGate. The FortiClient-FortiGate checks the port number for the SSL VPN service and user credentials to allow access. The SSL debug logs show the initial connection requested made by FortiClient to FortiGate. Then the SSL certificate negotiation takes place between FortiClient and FortiGate. The FortiClient side certificate information is located in the Installation directory\Fortinet\FortiClient folder.

DO NOT REPRINT
© FORTINET

FortiClient Features—SSL VPN Debug

- Debug
 - Change log level on FortiClient
 - Enable SSL VPN debug on FortiGate
 - `diag debug application sslvpn -l`
 - `diag debug application fndamd -l`
 - `diag debug enable -l`
- Capture network traffic on both FortiClient host and FortiGate
- You can also initiate SSL from the CLI
 - `FortiSSLVPNclient.exe /?`
 - `FortiSSLVPNclient.exe connect -h 172.17.61.48:443 -u test:111111 -c client_cert -i`
 - `FortiSSLVPNclient.exe disconnect`

FORTINET

52

You can run the real-time debug commands on FortiGate, which will show you similar information as on the FortiClient.

As a best practice, run the debug commands on FortiGate to compare them with the SSL VPN logs on FortiClient.

DO NOT REPRINT
© FORTINET

FortiClient Features—SSL Driver

- New SSL driver
 - New driver SSL VPN Virtual Ethernet Adapter is used by default
 - It solved SSL VPN disconnects at 98% issue
 - Log shows: `fortissl_connect: device=ftvnic`
- Old SSL driver
 - Old driver PPPoP WAN Adapter is also installed
 - To use old driver
 - Back up the configuration
 - Set `<use_legacy_ssl_adapter>` as 1
 - Restore the configuration
 - Restart FortiClient
 - Log shows: `fortissl_connect: device=fortissl`

FORTINET

53

Fortinet added its own SSL driver, or virtual adapter, to resolve issues related to the Windows PPP Wan Miniport Adapter. By default, FortiClient uses a new SSL driver. In logs, it shows as `fortissl_connect: device=ftvnic`.

The old SSL driver is also installed and appears as `fortissl_connect: device=fortissl`. You can use the old driver by making the following changes to the XML file:

- Back up the configuration
- Set `<use_legacy_ssl_adapter>` as 1
- Restore configuration
- Restart FortiClient

DO NOT REPRINT
© FORTINET

FortiClient Features—Application Firewall

- Only available for managed clients
- Disabled by default and hidden for standalone clients
- Configured on FortiGate or FortiClient EMS
- Files and drivers:
 - fcappdb.exe
 - fcappdb.db
 - xmlfw.dll
 - fortiws.exe
 - fortiapd.sys
 - fortifw2.sys
- vir_sig folder contains:
 - appsig.dat
 - ids.dat

FORTINET

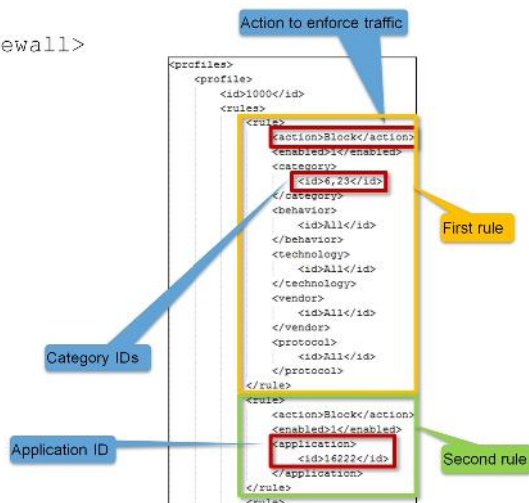
54

By default, application firewall is disabled and hidden for standalone clients, but you can configure and deploy it from FortiGate or FortiClient EMS. Application firewall uses an IPS engine, so it matches the patterns in the entire byte stream of the packet and requires multiple files and drivers.

FortiClient Features—Application Firewall

- Check XML configuration

- `<forticlient_configuration><vpn><firewall>`



FORTINET

55

The application firewall XML configuration elements can be grouped into two parts:

- General options:** Apply to all firewall activities.
- Profiles:** Defines the applications and the actions that apply to the firewall activities.

You can enable the `<candc_enabled>` XML configuration element by setting the value equal to 1, to detect a connection to a botnet command and control server. The `<default_action>` XML configuration element value is set to `pass`, which enforces the action to pass on traffic that doesn't match any defined profiles. You can change the default action to `block`, `reset`, or `pass`.

The `<profiles>` tag has a `<rules>` element. The `<rules>` element may, itself, have zero or more `<rule>` tags.

The following filter elements can be used to define applications in a `<rule>` tag:

```

<category>
<vendor>
<behavior>
<technology>
<protocol>
<application>
<popularity>

```

If the `<application>` element is present, all other sibling elements (listed above) will be ignored. If it is not present, a given application must match all of the provided filters to trigger the rule.

In the example shown on this slide, in the first rule, categories 6 and 23 are blocked, which corresponds to Proxy and Social.Media respectively. In the second rule, application 16779 is blocked which is Yahoo.Games. You can get the complete list of IDs corresponding to each category, behaviour, application from the FortiGate CLI.

DO NOT REPRINT
© FORTINET

FortiClient Features—Application Firewall

- FortiClient Logs
 - View recent violations on FortiClient GUI
 - Settings > Logging > Export logs**

Application Firewall Enabled
2 Violations (In the Last 7 Days)

```
xx/xx/20xx 9:05:05 AM Notice Firewall date=20xx-xx-xx time=09:05:04 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B103E8B05A77E38AD62028807 devid=FC78003611939390 fgtserial=FGW010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62401 direction=outbound destinationip=199.59.148.82 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=twitter vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy=default service=http

xx/xx/20xx 9:05:54 AM Notice Firewall date=20xx-xx-xx time=09:05:53 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B103E8B05A77E38AD62028807 devid=FC78003611939390 fgtserial=FGW010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62425 direction=outbound destinationip=104.25.62.28 remotename=N/A
destinationport=443 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked
utmevent=appfirewall threat=Proxy.Websites vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit
(build 9600)" usingpolicy=default service=https

xx/xx/20xx 9:28:23 AM Notice Firewall date=20xx-xx-xx time=09:28:22 logver=2 type=traffic level=notice sessionid=26453064
hostname=Win-Internal uid=C7F302B103E8B05A77E38AD62028807 devid=FC78003611939390 fgtserial=FGW010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62759 direction=outbound destinationip=208.71.44.31 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Yahoo.Games vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy=default service=http
```

- Common issues
 - Traffic is blocked, applications crash or are not categorized correctly

FORTINET

58

You can view the application violation logs directly on the FortiClient GUI or export logs by clicking **Settings > Logging > Export logs**.

In the example shown on this slide, FortiClient blocks two categories (proxy and Social.Media) and the application Yahoo.Games, when FortiClient inspects the traffic passing through it and, based on the matching rule, takes action. In this example, FortiClient blocks Twitter, proxy websites, and Yahoo.Games based on the defined rule.

Some common issues are blocked traffic, and applications that crash, or are not categorized correctly. Try to disable FortiClient features one-by-one, to make sure the issue is caused by the application firewall.

DO NOT REPRINT
© FORTINET

FortiClient Features—Vulnerability Scan

- Files and drivers
 - VCM daemon: Fcvbltscan.exe
 - VCM Engine: vcm2.exe
 - VCM signature: vcm.dat
- Registry
 - FA_VULN
 - FA_Schedule/000020
- Check XML configuration
 - <forticlient_configuration><vulnerability_scan>
- FortiClient Logs
 - View vulnerabilities detected on FortiClient
 - **Settings > Logging > Export logs**

```
<vulnerability_scan>
<enabled>1</enabled>
<scan_on_fgt_registration>0</scan_on_fgt_registration>
<scheduled_scans>
<schedule>
<enable_schedule>0</enable_schedule>
<repeat>0</repeat>
<type>24</type>
<day>3</day>
<time>19:30</time>
</schedule>
</scheduled_scans>
</vulnerability_scan>
```

```
xx/xx/20xx 10:07:25 AM Notice Vulnerability Scan id=96520 user=Administrator@TRAININGAD.TRAINING.LAB
msg="The vulnerability scan status has changed" status=started vulncat=N/A vulncvss=N/A vulnengine=N/A vulnid=N/A
vulnname=N/A vulnref=N/A vulnseverity=N/A

xx/xx/20xx 10:08:35 AM Notice Vulnerability Scan id=96521 user=Administrator@TRAININGAD.TRAINING.LAB
msg="A vulnerability scan result has been logged" vulncat=N/A vulncvss=N/A vulnengine=N/A vulnid=N/A
vulnname=ms_mirdous.Enabled.Cached.Login.Credential vulnref=www.fortinet.com/ids/VID20762 vulnseverity=Medium
```

FORTINET

57

The FortiClient vulnerability scan module can check your workstation for known system vulnerabilities. It uses various files and drivers to perform a vulnerability scan. You can scan your workstation when registering on FortiGate, or on a scheduled basis. Or you can run an on-demand scan directly from the FortiClient GUI and view the vulnerabilities found on the FortiClient console.

You can view the recent vulnerabilities detected directly on the FortiClient GUI, or you can export logs by clicking **Settings > Logging > Export logs**.

The vulnerabilities logs shows the status (started, cancelled) and also shows the name of the vulnerabilities detected, the severity, the vulnerabilities engine, and signatures used, and so on. It also provides a reference link, which provides the description, impact, and recommended actions for the vulnerability detected.

DO NOT REPRINT
© FORTINET

Vulnerability Scan—Debug

- Run debug from command line in elevated mode
 - Run VCM scan
 - `fcVlbtScan.exe -s fd_01 -d -n`
 - Run VCM patch
 - `fcVlbtScan.exe -s fd_01 -d -p path_to_install.json`
- Log file
 - `Forticlient_install_folder/logs/vcm/timestamp_folder`

FORTINET

50

You can run a vulnerability scan in debug mode from the command line in elevated mode. After running the commands shown on the slide, the log file will be available at the following location:

`Forticlient_install_folder/logs/vcm/timestamp_folder`

Example:

The following is a list of detected vulnerability JSON files, such as 36417.json, and so on:

- `Install.json:`
- `PatchedByProduct:.json`
- `Vcm scan and patch log: vcm_result.txt`

DO NOT REPRINT
© FORTINET

FortiClient Features—Telemetry and Compliance

- Telemetry file
 - FortiESNAC.exe
- Registry
 - FA_ESNAC
 - FA_Scheduler\000018
- XML
 - <forticlient_configuration><endpoint_control>
- Support the following functions:
 - Register to FortiClient EMS or FortiGate only
 - Register to one FortiGate on gateway IP list and monitored by EMS

```
<endpoint_control>
  <enabled>1</enabled>
  <socket_connect_timeouts>1:5</socket_connect_timeouts>
  <system_data>Enc </system_data>
  <disable_unregister>0</disable_unregister>
  <disable_fgt_switch>0</disable_fgt_switch>
  <show_bubble_notifications>1</show_bubble_notifications>
  <avatar_enabled>1</avatar_enabled>
```

FORTINET

59

FortiClient requires one file, FortiNAC.exe, for Telemetry.

The endpoint-related information is contained inside the <endpoint_control></endpoint_control> XML tags.

The <endpoint_control> XML tag contains configurations specifically related to endpoint telemetry.

It contains:

- Endpoint UI settings
- On-net addresses
- FortiGate details to register
- NAC rules
- Connections: user defined connections

DO NOT REPRINT
© FORTINET

Telemetry and Compliance (Contd)

- Compliance
 - Feature on top of Telemetry
 - FortiGate must be involved
 - Use the same
 - FortiESNAC.exe
 - Registry
 - XML
 - FortiGate provides compliance rule when compliance is enabled
 - Register to FortiGate only:
 - FortiClient will try to convert the compliance rule to FortiClient configuration on non-complaint machine
 - Register to one FortiGate on gateway IP list, and monitored by EMS:
 - FortiClient configuration comes from EMS
 - Admin will make FortiClient configuration consistent with FortiGate compliance rule

FORTINET

60

Compliance is the feature that runs on top of Telemetry. FortiGate must be involved. It uses the same FortiESNAC.exe, registry, and XML.

FortiGate provides the compliance rule when compliance enforcement is enabled

- Register to FortiGate only:
 - FortiClient will try to convert the compliance rule to the FortiClient configuration on a non-complaint endpoint
- Register to one FortiGate on gateway IP list, and monitored by EMS:
 - FortiClient configuration comes from EMS
 - Admin will make FortiClient configuration consistent with FortiGate compliance rule

- **FortiClient Logs**
 - Export logs from FortiClient GUI
 - **Settings > Logging > Export logs**
 - Change log level to **Debug** as no **Info** level logs for ESNAC

- | | | | | |
|-------------|----|-------|-------|---|
| 2:11:11.214 | PM | Debug | ESMBC | SetSecondaryDefault=20, SetSecondaryDefault = 200 |
| 2:11:11.214 | PM | Debug | ESMBC | min = 30 |
| 2:11:11.215 | PM | Debug | ESMBC | Timeout in select in SocketConnect |
| 2:11:11.215 | PM | Debug | ESMBC | Socket failed |
| 2:11:11.215 | PM | Debug | ESMBC | 102:163:1.154:0:0, Secondary = 0 |
| 2:11:11.215 | PM | Debug | ESMBC | UsePrivateIp=Decide |
| 2:11:11.215 | PM | Debug | ESMBC | Use Private IP |
| 2:11:11.215 | PM | Debug | ESMBC | W_GetSecondaryDefault false |
| 2:11:11.215 | PM | Debug | ESMBC | Start searching for FST |
| 2:11:11.215 | PM | Debug | ESMBC | SetSecondaryLabel |
| 2:11:11.214 | PM | Debug | ESMBC | Start searching for FST |
| 2:11:11.215 | PM | Debug | ESMBC | Searching Default ON |
| 2:11:11.214 | PM | Debug | ESMBC | SetSecondaryDefault=20, SetSecondaryDefault = 300 |
| 2:11:11.214 | PM | Debug | ESMBC | min = 30 |
| 2:11:11.215 | PM | Debug | ESMBC | Timeout in select in SocketConnect |
| 2:11:11.215 | PM | Debug | ESMBC | Socket connect failed |
| 2:11:11.215 | PM | Debug | ESMBC | 102:163:1.154:0:0, Secondary = 0 |

[illegible]

You can collect debug logs on an endpoint using the following steps:

- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Fortinet\FortiClient\FA_Scheduler\00018\cmd to FortiESNAC.exe -d (-p <password> is optional).

- For ESNAC, tmp esnac data.dat.

DO NOT REPRINT
© FORTINET

Knowledge Check

1. Which file is responsible for the FortiClient antivirus function?
✓ A. fmon.exe
B. fcappdb.exe
2. Why do you need to change the ESNAC.exe (Telemetry) log level?
✓ A. No information-level logs available
B. Limited details available

DO NOT REPRINT
© FORTINET

Lesson Overview

- ✓ How to Approach FortiClient Issues
- ✓ Common Issues with FortiGate and EMS
- ✓ FortiClient Troubleshooting
- ✓ FortiClient EMS Troubleshooting
- ✓ FortiClient Features Troubleshooting

FORTINET

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT
© FORTINET

Review

- ✓ How to Approach FortiClient Issues
- ✓ Common Issues with FortiGate and EMS
- ✓ FortiClient Troubleshooting
- ✓ FortiClient EMS Troubleshooting
- ✓ FortiClient Features Troubleshooting

FORTINET

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to approach FortiClient issues and common issues of FortiClient with FortiGate and EMS and, how to diagnose and troubleshoot FortiClient features.

DO NOT REPRINT
© FORTINET



FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.